FACULTAD DE TURISMO Y FINANZAS

GRADO EN FINANZAS Y CONTABILIDAD

De las Criptomonedas y Blockchain a DeFi. El caso del Mercado Blockchain de Futuros de AOVE

Trabajo Fin de Grado presentado por José Manuel Segura Rey, siendo el tutor del mismo el profesor Ismael Santiago Moreno.

Vº. Bº. Ismael Santiago Moreno

José Manuel Segura Rey

D. Ismael Santiago Moreno

D. José Manuel Segura Rey

Sevilla. Junio de 2021

GRADO EN FINANZAS Y CONTABILIDAD

FACULTAD DE TURISMO Y FINANZAS

TRABAJO FIN DE GRADO

CURSO ACADÉMICO [2020-2021]

TÍTULO:

DE LAS CRIPTOMONEDAS Y BLOCKCHAIN A DEFI. EL CASO DEL MERCADO BLOCKCHAIN DE FUTUROS DE AOVE

AUTOR:

JOSÉ MANUEL SEGURA REY

TUTOR:

Dr. D. ISMAEL SANTIAGO MORENO

DEPARTAMENTO:

ECONOMÍA FINANCIERA Y DIRECCIÓN DE OPERACIONES

ÁREA DE CONOCIMIENTO:

ECONOMÍA FINANCIERA Y CONTABILIDAD

RESUMEN:

El desarrollo de la tecnología blockchain está provocando una serie de cambios en los servicios financieros que jamás hubiéramos imaginado. Esta tecnología disruptiva es la base del protocolo DeFi, proporcionando importantes ventajas competitivas, las cuales están permitiendo una expansión de estos protocolos.

El nacimiento de DeFi como lo conocemos comenzó en la blockchain de Ethereum, con el objetivo de construir un mejor panorama financiero hecho posible gracias a la llegada de internet y la tecnología blockchain.

Blockchain juega un papel importante en lo que se denomina la nueva economía blockchain, la cual es la siguiente fase de la evolución de internet a la que denominamos la era de la descentralización.

Bitcoin fue el primer caso de uso de la tecnología Blockchain, dando lugar a la primera criptomoneda sin ningún tipo de respaldo bancario o gubernamental. Poco después

apareció Ethereum, que observó que la cadena de bloques podría ser usada más allá de tan solo como una moneda, consolidándose como la plataforma para implementar servicios financieros descentralizados. Debido a la volatilidad a la que están sometidas las criptomonedas tuvo lugar la aparición de las stablecoins, para así de esta forma evitar las fuertes variaciones de precios a la que estas están sometidas.

Gracias a la cadena de bloques, podemos resolver problemas económicos y financieros como los que presenta el sector del aceite de oliva, esto es posible gracias a la aparición del mercado de futuros del aceite de oliva, el cual está totalmente descentralizado.

PALABRAS CLAVE:

Bitcoin; Ethereum; DeFi; blockchain; smart contract.

ÍNDICE

CAPÍTULO 1: INTRODUCCIÓN

1.1. JUSTIFICACIÓN

Internet ha permitido que millones de personas puedan acceder a una mayor cantidad de información, mejorando de esta forma la educación y calidad de vida de muchos pueblos de alrededor del mundo. Del mismo modo que internet permitió este intercambio de ideas, las criptomonedas y blockchain proporcionaran a las personas acceso a un nuevo modelo económico y financiero descentralizado. Aquí es donde entra en juego DeFi (Finanzas descentralizadas), el cual, actualmente es uno de los sectores de más rápido crecimiento en el espacio blockchain y criptomonedas.

Ante este nuevo panorama financiero, DeFi pretende convertir las estructuras de finanzas centralizadas que tenemos ahora, en estructuras descentralizadas, sin intermediarios de confianza, ejecutada a través de contratos inteligentes dentro de una blockchain, donde todo queda registrado de forma transparente.

Para aquellos que sostienen una postura más liberal a nivel económico dentro del capitalismo, DeFi, supone un paso adelante para evitar la regulación de los gobiernos, realizar pagos e inversiones internacionales sin tanta burocracia, evitar costes y tiempo, así como un mayor acceso a los servicios financieros, con mayores niveles de confianza y transparencia.

La relevancia que está teniendo DeFi en el sector financiero y el rápido crecimiento de este ecosistema, es lo que nos lleva a estudiar más detalladamente en qué consisten las finanzas descentralizadas, así como su disruptiva tecnología, la cual es el gran soporte de dicho ecosistema.

A nivel personal, DeFi llama mi atención, ya que es un mundo distinto y diverso que no guarda relación con el sistema que conocemos, en el que un préstamo es otorgado por una entidad financiera, o donde las monedas se pueden tener de forma física y están controladas bajo un estado. Detrás de DeFi no se encuentra ningún banco central o gobierno que respalde el valor de las monedas, o una entidad financiera encargada de concedernos un préstamo. La confianza en el ecosistema lo genera la propia tecnología y el conocimiento en profundidad de su funcionamiento.

Por ello, este el punto de inicio donde mi interés por DeFi y su funcionamiento comienza, convirtiéndose en mi elección para el trabajo de fin de grado.

1.2. OBJETIVOS

Este trabajo pretende realizar un estudio del ecosistema DeFi (Finanzas descentralizadas), así como de sus principales protocolos.

Para alcanzar este objetivo general o estratégico, vamos a definir unos objetivos tácticos que nos faciliten el desarrollo de nuestro trabajo.

En primer lugar, se realizará un estudio de Bitcoin, el cual ha sido pionero en el uso de la tecnología de la cadena de bloques y posteriormente se estudiará Ethereum, que fue quien observó que la cadena de bloques se podía utilizar más allá de tan solo como una moneda.

A continuación, nos adentraremos en conocer la cadena de bloques, así como las propiedades que esta presenta.

Seguidamente nos adentraremos en el ecosistema DeFi, para conocer así en que consiste y sus principales protocolos.

Finalmente, mostraremos un caso del impacto y la importancia que tiene la cadena de bloques en el sector del aceite de oliva.

1.3. ESTRUCTURA

El trabajo constará en un primer capítulo de la moneda electrónica Bitcoin, donde conoceremos sus antecedentes, como funciona, y la oferta y demanda de esta.

Un segundo capítulo donde conoceremos Ethereum, su funcionamiento y la importancia de los contratos inteligentes y aplicaciones descentralizadas dentro de esta.

Un tercer capítulo, donde hablaremos de la tecnología que sustenta a todo el ecosistema DeFi, conocida como blockchain.

Un cuarto capítulo donde conoceremos el concepto de la nueva economía blockchain, así como los principios y leyes en las que esta se basa.

Un quinto capítulo, el cual nos introduce en DeFi, a través de una explicación y de los objetivos que busca dicho ecosistema.

Un sexto capítulo, donde conoceremos que son las stablecoins, en concreto Dai.

Un séptimo capítulo, donde analizaremos los protocolos líderes en el mercado DeFi.

Un octavo capítulo, en el cual mostramos un caso de los beneficios que puede causar la introducción de blockchain y la creación de un mercado de futuros descentralizado en el sector del aceite de oliva.

Para finalizar, obtendremos unas conclusiones globales que hemos extraído con la realización del trabajo.

1.4. METODOLOGÍA

La metodología llevada a cabo en este trabajo se basa en la revisión bibliográfica de autores nacionales y extranjeros que han investigado el fenómeno de blockchain.

En el subepígrafe 4.1. se ha procedido a la revisión bibliográfica del concepto blockchain o cadena de bloques, atendiendo a las diversas aportaciones conceptuales de diversos autores, tanto nacionales como extranjeros, para que finalmente, a modo de síntesis, el autor de este TFG aporte su propia definición.

CAPÍTULO 2: BITCOIN

2.1. ANTECEDENTES

Bitcoin es la criptomoneda de moda, sin embargo, no fue algo que se improvisase de la noche a la mañana, y otros antes que Satoshi Nakamoto, idearon sistemas que solamente Bitcoin parece haber sido capaz de popularizar y hacer llegar al gran público. No obstante, todos perseguían el mismo objetivo: conseguir, sin necesidad de un tercero de confianza, que en el dinero electrónico funcionasen la anonimidad y la descentralización. (Márquez Solís, 2016)

En 2008, se inicia la historia de Bitcoin cuando Satoshi Nakamoto publica por primera vez su *Libro blanco de la red Bitcoin* y lo envía a un pequeño grupo de defensores de la privacidad y especialistas en ciencias informáticas y criptográficas. Este grupo estaba formado por los remitentes del mailing list del movimiento cypherpunk. Algunos de los participantes de esta lista mantuvieron el anonimato. Sin embargo, otros son públicamente conocidos y son activos artífices en la creación de herramientas de software para la mejora de la privacidad.

El movimiento cypherpunk entendía y entiende la privacidad como el legítimo derecho que tiene cada ciudadano del mundo de revelar solo la información que desea, como queda expresado en el *Manifiesto Cypherpunk* de Eric Hughes: << La privacidad es el poder de revelarse selectivamente al mundo>>. Este movimiento más filosófico que tecnológico, ante la amenaza que suponía el control y la censura ejercida por los gobiernos y las autoridades centrales sobre el desarrollo de la información, de la tecnología y el intercambio de valor, llevo a sus miembros a enarbolar la bandera de la privacidad.

Las ideas y el grupo ya habían estado gestándose desde los años ochenta, especialmente impulsados por el trabajo de David Chaum, uno de los primeros especialistas en preocuparse por la privacidad en las transacciones financieras. Chaum está acreditado como el inventor del dinero digital seguro por sus trabajos de investigación. En 1990 Chaum fundó DigiCash, una compañía de dinero efectivo cuyo primer pago electrónico fue enviado en 1994; en 1999, abandonaría esta empresa.

Bitcoin podría llegar a considerarse como un producto cypherpunk, no solo como síntesis de varios proyectos inspirados en este movimiento, sino también en la realización de varios de sus ideales. Como se puede leer en el manifiesto cypherpunk: << Un sistema anónimo permite a los individuos revelar su identidad cuando se desea y solo cuando se desea; esta es la esencia de la privacidad>>.

Con Bitcoin Nakamoto plantea la solución de una red de intercambio de valor, descentralizada y de alcance global, tejida como el mosaico de varios proyectos que los cypherpunks habían madurado durante años, los cuales vamos a describir a continuación. Bitcoin heredó la tecnología de la prueba de trabajo de Adam Back. Si bien Hashcash fue ideado para potenciar sistemas *antispam,* el funcionamiento de la prueba de trabajo que utiliza tiene bastante similitud con el diseño del algoritmo de minado de Bitcoin.

El b-money de Wei Dai tiene muchas similitudes con el borrador de Bitcoin. Como Bitcoin, b-money requería una cantidad específica de trabajo computacional, el cual debía ser verificado por los usuarios, que tenían que actualizar un sistema contable público descentralizado. Además, quienes participaban de prueba de trabajo del sistema recibían una recompensa por su actividad y se autenticaban con hashes criptográficos (una huella digital dactilar, para que nos entendamos). A diferencia de Bitcoin, b-money nunca llegó a funcionar.

Nick Szabo creo Bit Gold, que consistía en un sistema de intercambio de valor que disponía de un novedoso sistema de consenso de red inspirado en la teoría de juegos y que evitaba la posibilidad de realizar el doble gasto con el mismo dinero en la red gracias a la resolución un problema matemático.

Hal Finney colaboró notablemente en el desarrollo de un sistema de pruebas de trabajo reutilizables totalmente funcional antes de Bitcoin, además de su activa participación en los primeros días de Bitcoin, para lo que fue uno de los más activos interlocutores de Nakamoto y uno de los primeros en descargarse y utilizar la primera versión del cliente Bitcoin.

La red Bitcoin se puso en marcha el 3 de enero de 2009 con el bloque génesis, en el cual Satoshi Nakamoto plasmaba la idea que tenía sobre la crisis financiera de 2008 y como propuso una alternativa a la misma. En un extracto oculto de dicho bloque, se podía leer un título extraído del periódico británico *The Times*, que decía lo siguiente: << The Times 03 de enero de 2009. Canciller al borde del segundo rescate para bancos>>. Con este mensaje, se daba inicio a Bitcoin y se nos mostraba las intenciones de Satoshi ante esta noticia, que indicaba que el gobierno de Estados Unidos rescataba el sistema financiero con setecientos mil millones de dólares. (Santiago Moreno, 2019)

2.2. ¿QUÉ ES BITCOIN?

Bitcoin es una *moneda electrónica* descentralizada, concebida en 2009 por quien se ha dado a conocer como Satoshi Nakamoto (aunque su verdadera identidad se desconoce). El nombre de Bitcoin se aplica también al *software libre* diseñado por Nakamoto para la gestión de dicha moneda, y a la red P2P (peer to peer) que le da soporte.

El funcionamiento de Bitcoin no depende de una institución central, sino de una *base de datos distribuida* conocida como cadena de bloques o blockchain. El software emplea la *criptografía* para proveer funciones de seguridad básicas, como garantía de que los bitcoins solo puedan ser gastados por su dueño, y nunca más de una vez.

El diseño de Bitcoin permite poseer y transferir valor entre cuentas públicas de forma potencialmente anónima. El mayor logro de Nakamoto ha sido el haber resuelto el problema de doble gasto en un sistema descentralizado. Para evitar que un mismo Bitcoin sea gastado más de una vez por la misma persona, la red se vale de un *servidor de tiempo distribuido,* que ordena secuencialmente las transacciones e impide su modificación. Esto se logra por medio de pruebas de trabajo encadenadas, realizadas por los mineros a cambio de una recompensa en bitcoins.

Hasta la fecha, no se ha dado ningún caso de doble gasto, pero es cierto que un ataque informático de este tipo es posible, siempre y cuando el atacante controle al menos el 51% del poder computacional que protege a la red. Sin embargo, engañar a la red el tiempo suficiente como para llevar a cabo un único doble gasto implicaría una inversión tan descomunal, y una organización tan compleja que desde un punto de vista económico sería más provechoso poner esos recursos a trabajar bajo las reglas del protocolo Bitcoin. (González Otero et al., 2013)

2.2.1. Funcionamiento de Bitcoin

El funcionamiento de Bitcoin es posible gracias a la blockchain o cadena de bloques de este, la cual es una tecnología de contabilidad distribuida pública en donde se registran todas las transacciones y que funciona como una base de datos. Esta contabilidad pública trabaja con una red distribuida de ordenadores (o nodos); es decir,

sin requerir ningún ente central que asuma el rol de intermediario. La cadena de bloques funciona igual que un libro mayor de contabilidad en donde los apuntes son públicos y descentralizados. Blockchain está formado por una cadena de bloques configurada exclusivamente para evitar su modificación una vez que los datos han sido validados y publicados.

La descentralización funciona gracias a que las transacciones incluidas en los bloques son creadas por los integrantes del sistema. Todas las transacciones son registradas y transmitidas a todos los nodos de la red. Así, todos los integrantes tienen la misma información.

Un nodo es un ordenador conectado a la red que emplea un programa informático para almacenar y distribuir una copia actualizada, en tiempo real, de la blockchain. Las transacciones se realizan desde monederos electrónicos o wallets, los cuales consisten en archivos encriptados que funcionan de forma similar a una cuenta bancaria. Un monedero electrónico es un conjunto de clave pública y privada controladas por un software. La clave pública es una cadena alfanumérica de treinta y cuatro caracteres de longitud que componen lo que se conoce como un hash criptográfico. Esta es la dirección de Bitcoin, que hace las veces de número de cuenta. De esta forma para que un usuario envíe Bitcoin a otro y los reciba, previamente debe haberle dado la clave pública.

La clave privada es una cadena de sesenta y cuatro caracteres de longitud que prueba que eres el dueño de la clave pública. Además, es necesaria para decirle a la red que estas enviando bitcoins a otro monedero. Esta clave sirve para autorizar transacciones desde el monedero electrónico, para lo que se emplea en todo este proceso la criptografía asimétrica.

Un bloque es un conjunto de transacciones confirmadas. Cada bloque es una parte de la cadena con los siguientes elementos básicos: un código alfanumérico que enlaza con el bloque anterior, un conjunto de transacciones y otro código alfanumérico que enlazará con el bloque posterior. Un bloque debe ser añadido a la cadena mediante un hash, que es una huella dactilar de un documento y que se genera mediante una serie de operaciones matemáticas.

Los mineros, por su parte, se dedican a verificar las transacciones que se están produciendo en la red. Estos cumplen dos funciones: crear nuevos bitcoins por cada bloque que se mina y asegurar que las transacciones sean veraces y legítimas. Comprueban que la serie temporal es correcta y que todas las transacciones dentro del bloque son válidas. En la actualidad, los mineros se agrupan en pools de minería (un conjunto de mineros) que trabajan en conjunto para resolver un bloque. Entre ellos, se reparten las compensaciones obtenidas en proporción a la capacidad de cómputo aportada por cada uno de los mineros que forman el pool. Actualmente, sin un grupo de minería, es difícil llegar a ganar alguna recompensa. (Santiago Moreno, 2019)

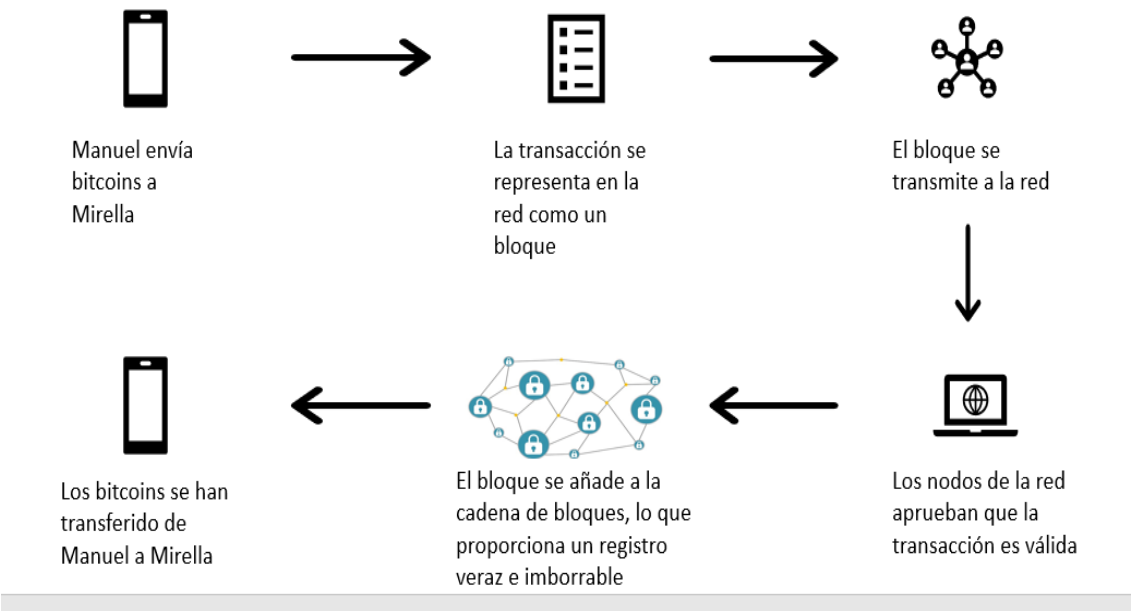

Figura 2.1. Proceso de una transacción con Bitcoin

Fuente: Elaboración propia a partir de la información contenida en La Nueva Economía Blockchain y Criptomonedas en 100 preguntas (Santiago Moreno, 2019)

En la imagen podemos observar el proceso de transacción de un Bitcoin. Centrándonos en el ejemplo, Manuel da la orden de enviar sus bitcoins a Mirella, una vez dada la orden, la operación se registra en la red y los nodos compiten entre sí para resolver un problema y validar dicha transacción, el ganador crea un nuevo bloque que incluye esta y otras transacciones, los demás nodos validan que el bloque se haya creado correctamente y propagan esta información a los demás nodos de la red. De esta forma un nuevo bloque se ha creado y todos los nodos eventualmente tendrán la misma información, de esta manera Mirella puede validar consultando a cualquier nodo que su cuenta en Bitcoin ha sido actualizada.

2.3. OFERTA Y DEMANDA MONETARIA DE BITCOINS

Una vez que ya hemos contextualizado su origen y su funcionamiento, pasamos a centrarnos en su implicación económica, para lo cual vamos a estudiar cómo se forma su oferta monetaria y los determinantes de su demanda.

2.3.1. Oferta monetaria de Bitcoins

A diferencia de la moneda convencional, Bitcoin no puede ser controlado por ninguna autoridad debido a su naturaleza descentralizada. La expansión de la base monetaria está predeterminada por el software de Bitcoin y es conocida por todos, de manera que no es posible afectar el poder adquisitivo de los usuarios manipulando la cantidad de bitcoins en circulación.

Aproximadamente seis veces por hora, la red Bitcoin crea y distribuye un lote de nuevos bitcoins a quien esté ejecutando el software para generar bitcoins (software de minería). Generar bitcoins es conocido como <<minar>>, un término que remite a la minería de metales preciosos. La probabilidad de que un usuario reciba un lote depende del poder computacional con el que contribuye a la red en relación al poder computacional de todos los otros nodos combinados.

El primer nodo generador en encontrar la solución al problema criptográfico que presenta el bloque-candidato es el que obtiene un nuevo lote de bitcoins. Los <<mineros>> también pueden unirse por medio de internet para generar bitcoins en grupo, formando un pool minero. (González Otero et al., 2013)

La cantidad de bitcoins creada por lote nunca es ni será mayor a 50 BTC y los premios (el número de bitcoins por lote) están programados para disminuir con el paso del tiempo, este proceso recibe el nombre de Halving, el cual sucede cada 210.000 bloques, estos se producen en un plazo de más o menos cuatro años. En la actualidad la recompensa se encuentra en 6.25 BTC. Reduciendo la recompensa para los mineros, se limita la circulación de bitcoins y, por tanto, se limita la oferta del activo, la cual es de 21 millones de bitcoins. De modo que para que les sea rentable a los mineros seguir minando, el precio de Bitcoin en el medio-largo plazo debe de subir. (*Cointelegraph.Com*)

Para que un bloque sea generado cada diez minutos, el protocolo actualiza cada dos semanas la dificultad del problema que todos los nodos generadores están intentando resolver, ajustándola al poder computacional de toda la red. (González Otero et al., 2013)

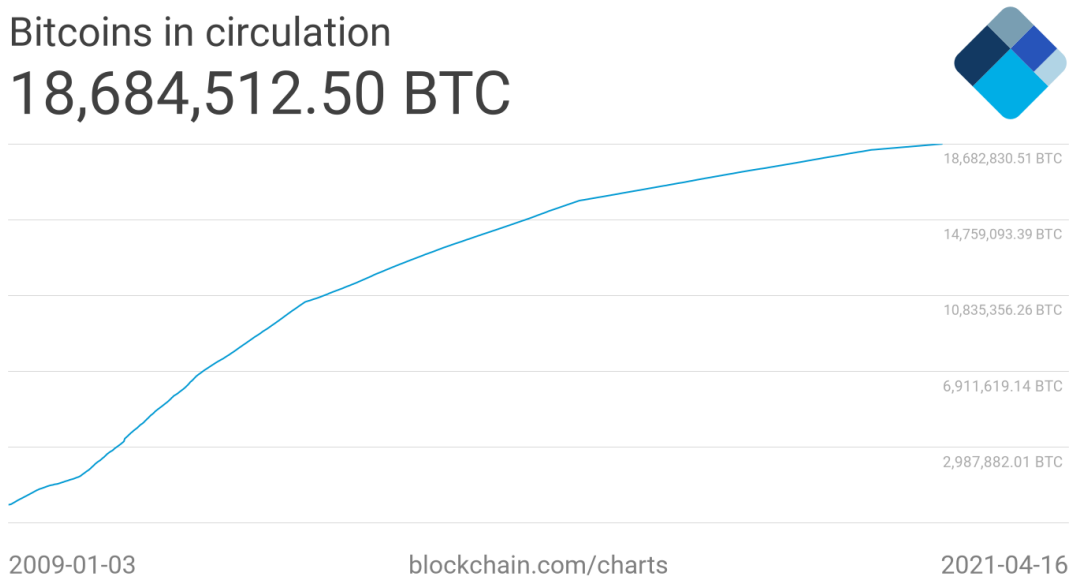

Figura 2.2. Número de Bitcoins en circulación

Fuente: (*Blockchain.Com*)

En la actualidad como podemos ver en la gráfica el número de Bitcoins en circulación el día 16/04/2021 es de 18.684.512,50. Este número se calcula a partir de la recompensa teórica definida por el protocolo Bitcoin.

2.3.2. Demanda monetaria de Bitcoins

Una vez que hemos aclarado la oferta monetaria de bitcoins, procederemos a hablar de la demanda monetaria de este. Para ello, la mejor forma de explicarlo es a través de la interrelación entre la oferta y demanda.

Debido al carácter descentralizado que tiene Bitcoin, la moneda no posee un "respaldo" desde el punto de vista financiero tradicional. Ello implica que no podemos

valorar su precio por indicadores como el PIB, Inflación o desarrollo económico que tenga un país en específico.

Pese a no tener un respaldo desde el punto de vista financiero, podemos afirmar que es más segura que el resto de las monedas FIAT con sus sistemas de hiperinflación, producción inorgánica y distribución poco transparente.

Como no existe una autoridad central confiable que determine el precio, este lo determinan los miembros del mercado que compran y venden bitcoin a cambio de su moneda local.

Los mercados determinan tendencias por medio de la oferta y la demanda, es decir, por el interés de comprar o vender un objeto. Si el mercado tiene mucho interés en adquirir determinado objeto y dicho objeto se encuentra limitado, el precio de dicho objeto aumentará. Es lo que llamamos una demanda superior a la oferta existente dentro del mercado.

Por otro lado, si la oferta de determinado producto aumenta por encima de la demanda real de dicho producto dentro del mercado, su precio tenderá a bajar. La oferta puede aumentar por muchas razones: Exceso de producción, imposibilidad de limitar el acceso de la población al producto, etc.

En el caso del Bitcoin, su oferta está ya determinada desde un comienzo. 21 millones de Bitcoins el tope máximo de producción que se verá dentro de la red Blockchain de esta criptomoneda. Con una oferta delimitada, lo que nos va a interesar para marcar el precio será su demanda dentro de los mercados.

Los mercados que marcan los precios del Bitcoin son los Exchanges o Casas de Intercambio que sirven como plataforma para intercambiar moneda FIAT por Bitcoin. En estos espacios, las personas colocan sus ofertas tanto para comprar o para vender, lo pueden hacer libremente sin ningún tipo de limitación.

Al ser un mercado mundial, son muchos los elementos que pueden influenciar su precio tanto para arriba como para abajo. Algunos de los elementos más comunes que afectan a su precio son:

- *Desarrollo tecnológico*:

  Los avances y desarrollos tecnológicos que tenga el Bitcoin impactan positivamente en sus precios. Desarrollos como el Lightning Network y demás avances en materia de usabilidad, escalabilidad y seguridad del Bitcoin permiten que la moneda pueda ser adoptada de una manera más fácil por las personas y ello implica que aportará una mayor demanda del activo.

  Por otro lado, si se conocen estudios y evaluaciones que determinen que la red Blockchain de Bitcoin no es segura y que puede ser hackeable, ello impactará negativamente el precio del activo puesto que los poseedores querrán vender el activo y dentro del mercado existirán más vendedores que compradores.

- *Mayores niveles de aceptación y usabilidad*:

  La tienda on-line de Amazon anunció que se podía pagar en ella con nuestros Bitcoins gracias a Lightning Network y ello tuvo una implicancia efectiva para el precio de la moneda. Esto afecto de manera positiva a la moneda ya que implica un mayor uso de la misma dentro de un mercado grande de usuarios.

  Lo mismo sucede cuando se refleja que hay un mayor grado de aceptación de la moneda dentro del mercado financiero. Podemos verlo cuando vemos que una cadena de negocios o un comercio en particular anuncia al mundo que

acepta como forma de pago el Bitcoin, aquí podemos apreciar como la moneda empieza a abrirse más entre el público y su usabilidad aumenta.

- *Trastornos en el mercado tradicional:*

  Muchos inversores tradicionales han visto al Bitcoin como una inversión alternativa cuando los mercados tradicionales (acciones, divisas o materias primas) se encuentran errantes o estiman que hay amenazas serias que afectarán su correcto desarrollo. (*Cointelegraph.Com*)

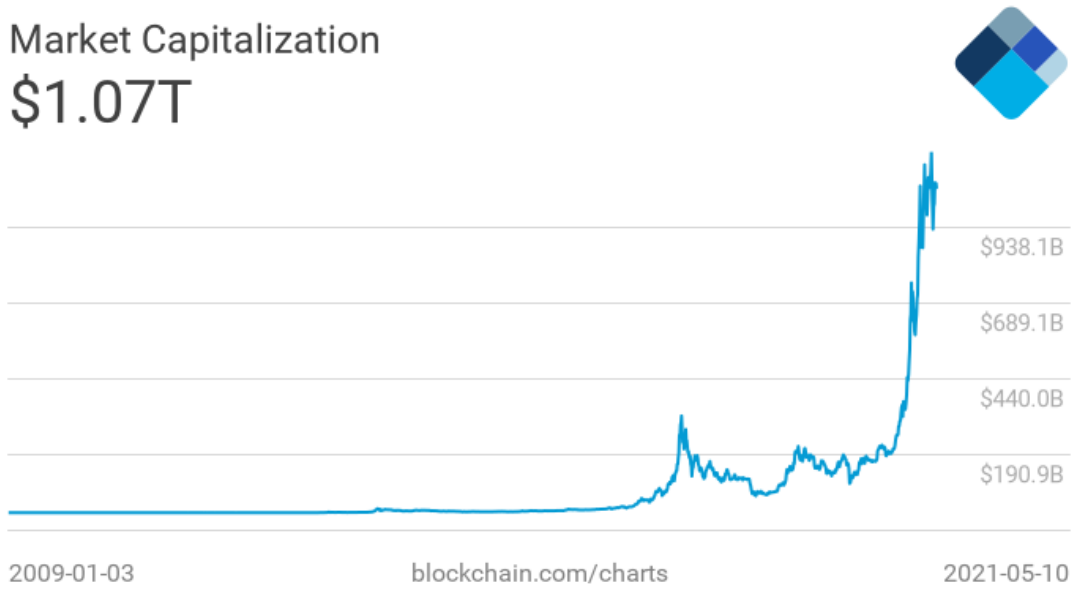

Figura 2.3. Capitalización de mercado de Bitcoin

Fuente: (*Blockchain.Com*)

Esta gráfica ilustra la capitalización de mercado de Bitcoin, la cual se encuentra en la fecha de escritura en 1,056,524,480,144 dólares. Como podemos ver el precio de Bitcoin se mantuvo sin variaciones durante los tres primeros años, en 2017-2018 hubo un repunte, corrigiendo su cotización tras este incremento. Sin embargo, desde mediados de 2020 ha sufrido un fuerte incremento en su cotización unido a una altísima volatilidad.

CAPÍTULO 3: ETHEREUM

3.1. ¿QUÉ ES ETHEREUM?

La plataforma Ethereum fue creada en 2015 por el programador Vitalik Buterin, con la perspectiva de crear un instrumento para aplicaciones descentralizadas y colaborativas. (*Www.Ig.Com*)

Ethereum es una red y plataforma global de código abierto para ejecutar nuevos tipos de aplicaciones. Ethereum se conoce como una “plataforma de contrato inteligente” donde estas aplicaciones pueden programar la transferencia de valor de una dirección a otra cuando se cumplen ciertas condiciones.

La ejecución de estos programas requiere el uso de una criptomoneda nativa llamada éter (ETH) (Demirors & Sheffield, 2020), es como el dinero y se puede utilizar para transacciones diarias similares a Bitcoin. Puede enviar ether a otra persona para comprar bienes y servicios basados en el valor de mercado actual. La cadena de bloques Ethereum registra la transferencia y garantiza el final de la transacción.

Además, ether también se utiliza para pagar la tarifa que permite que los contratos inteligentes y Dapps se ejecuten en la red Ethereum. Esta tarifa es conocida como Gas, la cual se refiere a la unidad de medida sobre la cantidad de esfuerzo computacional necesario para ejecutar una operación. Cuanto más compleja sea la operación de ejecución, más Gas se requiere para cumplir con esa operación.

El precio del gas puede fluctuar en función de la demanda de la red. Si hay más personas interesadas en usar la red Ethereum, debido a la limitada cantidad de recursos informáticos en la red, el precio del gas puede aumentar. Por el contrario, cuando la red esta infrautilizada, el precio de mercado del gas disminuiría.

Por otro lado, Ethereum se puede utilizar para otras dos funciones: crear organizaciones autónomas descentralizadas (DAO) o emitir otras criptomonedas.

Una DAO es una organización totalmente autónoma que no se rige por una sola persona, sino que se rige a través de código. El código se basa en contratos inteligentes y permite a las DAO reemplazar cómo se ejecutan normalmente las organizaciones tradicionales. A medida que se ejecuta el código, estaría protegido de la intervención humana y funcionara de manera transparente. No habrá ningún efecto por ninguna entrada externa. Las decisiones de gobierno o las resoluciones se decidirán a través de la votación simbólica de DAO.

En cuanto a la emisión de monedas, Ethereum se puede utilizar como una plataforma para crear otras criptomonedas. Actualmente hay dos protocolos populares para tokens en Ethereum Network: ERC-20 y ERC-721. ERC-20 es un estándar de protocolo que define reglas y estándares para la emisión de tokens en Ethereum. Las fichas ERC-20 son fungibles, lo que significa que son cambiables y del mismo valor. Por otro lado, las fichas ERC-721 no son fungibles, lo que significa que es completamente única y no intercambiable. Una comparación simple sería pensar en ERC-20 como dinero y ERC-721 como coleccionables. (Lau et al., 2020)

3.1.1. Funcionamiento de Ether

Ether, como otras criptomonedas, utiliza un libro digital compartido donde se registran todas las transacciones. Es de acceso público, completamente transparente y muy difícil de modificar a posteriori.

Este ‘libro contable digital’ se denomina blockchain o cadena de bloques, y se construye a través del proceso de minería de datos.

Los mineros son los responsables de verificar grupos de transacciones de ether para formar "bloques" y codificarlos resolviendo complejos algoritmos. Estos algoritmos pueden ser a su vez más o menos difíciles, como forma de mantener cierta constancia en el tiempo de procesamiento de los bloques (alrededor de uno cada 14 segundos).

Los nuevos bloques se enlazan entonces a la cadena de bloques anterior y el minero en cuestión recibe una recompensa, es decir, un número fijo de *tokens* de ether. Normalmente son 5 unidades de ether, aunque esta cifra puede verse reducida si la criptomoneda continúa subiendo.

3.1.2. Funcionamiento de Ethereum

El blockchain de Ethereum es muy similar al de bitcoin, pero su lenguaje de programación les permite a los desarrolladores crear software a través del cual gestionar las transacciones y automatizar ciertos resultados. Este software se conoce como contrato inteligente.

Si un contrato tradicional describe los términos de una relación, un contrato inteligente se asegura de que esos términos se cumplen escribiéndolos en código. Son programas que automáticamente ejecutan el contrato una vez que las condiciones predefinidas se cumplen, eliminando el retraso y el coste que existe al ejecutar un acuerdo de manera manual. (*Ig.Com*)

3.2. SMART CONTRACTS

Con la revolución tecnológica que supone blockchains y sus propuestas, gracias a Vitalik Buterin llega la posibilidad con la que no solo es posible tener una red pública, descentralizada, segura y confiable, sino que permite la ejecución de códigos y de programas de forma descentralizada y la implementación de los contratos inteligentes.

Un contrato inteligente o Smart contracts es cualquier contrato que se ejecuta por sí mismo automáticamente sin la mediación de terceros. Además, se escriben como programas informáticos en lugar de ser escritos en lenguaje legal sobre documentos impresos. El programa puede definir reglas y consecuencias estrictas del mismo modo que lo haría un documento legal tradicional, pero a diferencia de los contratos tradicionales, también puede tomar información que se le proporcione y tenga en cuenta para procesarla según las reglas establecidas dentro del contrato y con relación a esto operar y producir un resultado. (Ocariz, 2018)

Los contratos inteligentes funcionan en el principio de “si esto, entonces eso”. Siempre que se cumpla una determinada condición, el contrato inteligente llevará a cabo la operación según lo programado.

Si múltiples contratos inteligentes se combinan para operar entre sí, surge lo que se conocería como aplicación descentralizada (Dapp).

Las Dapps son interfaces que interactúan con la cadena de bloques a través del uso de contratos inteligentes. Las Dapps se ven y se comportan como aplicaciones web y móviles regulares, excepto que interactúan con una cadena de bloques y de diferentes maneras. Algunas de las maneras incluyen requerir ETH para utilizar la Dapp y almacenar datos.

Los beneficios que presentan las Dapps son los siguientes:

- *Inmutabilidad*: Nadie puede cambiar ninguna información una vez que está en la cadena de bloques.
- *A prueba de manipulaciones*: Los contratos inteligentes publicados en la cadena de bloques no se pueden manipular sin alertar a todos los demás participantes en la cadena de bloques.
- *Transparente*: Los contratos inteligentes que alimentan las aplicaciones de comandos son abiertamente auditables.
- *Disponibilidad*: Mientras la red Ethereum siga siendo activa, las Dapps construidas en ella permanecerán activas y utilizables.

Mientras que las desventajas en las que incurren las Dapps son las siguientes:

- *Inmutabilidad:* Los contratos inteligentes son escritos por humanos y solo pueden ser tan buenos como la persona que los escribió.
- *Transparente:* Los contratos inteligentes abiertamente auditables también pueden convertirse en vectores de ataque para los piratas informáticos, ya que pueden ver el código.
- *Escalabilidad:* En la mayoría de los casos, el ancho de banda de una Dapp se limita a la cadena de bloques en la que reside. (Lau et al., 2020)

Figura 3.4. Capitalización de mercado de Ethereum

Fuente: (*Coinmarketcap.Com*)

En este gráfico podemos apreciar la capitalización de mercado que ha tenido Ethereum desde su inicio. Gran parte de este crecimiento se debe a la importancia que tiene dicha plataforma para el ecosistema DeFi, el cual entraremos en profundidad más adelante.

CAPÍTULO 4: BLOCKCHAIN

En los capítulos anteriores se ha abordado el concepto de Bitcoin y Ethereum, así como su funcionamiento. Puesto que la tecnología blockchain nació como la mano derecha de Bitcoin y Ethereum ha expandido las capacidades que ofrecía Bitcoin gracias a los contratos inteligentes y las Dapps, es necesario adentrarnos en el concepto de la cadena bloques, así como sus propiedades y las diferentes tipologías que existen de esta.

4.1. DEFINICIÓN DE BLOCKCHAIN

Como ya indicábamos en el subepígrafe 1.4. relacionado con la metodología desarrollada basada en la revisión bibliográfica del término blockchain, hemos recogido las diversas definiciones aportadas por los autores expertos, tanto nacionales y extranjeros, para que finalmente, a modo de síntesis, aportamos nuestra propia definición, basada en la investigación desarrollada sobre este fenómeno de la cadena de bloques y el impacto que ya está teniendo en la economía y en las actuales finanzas internacionales.

Para Nakamoto (2008), blockchain es un servidor de tiempo distribuido, que identifica y ordena secuencialmente las transacciones e impide su modificación.

Según Antonopoulos (2014), la cadena de bloques es un libro contable global de todas las transacciones, aceptada por todo el mundo en la red Bitcoin, como registro de autoridad de la propiedad. La estructura de datos de la cadena de bloques es una lista ordenada de bloques de transacciones, enlazada hacia atrás en el tiempo.

BBVA innovation Center (2016), define blockchain como una base de datos con información horaria estampada e inmutable de cada transacción, que se replica en servidores de todo el mundo.

Para López y Mora (2016), la blockchain es un gran libro de contabilidad que se va incrementando, conforme se va produciendo movimientos (y estén escritos), éstos nunca podrán ser modificados por nadie, lo que le da legitimidad y la posibilidad de gestionar transacciones a través de la red, entre personas que no se conocen. Este libro contable está completamente distribuido y se actualiza constantemente con las nuevas entradas contables, las cuales se agruparán en bloques, antes de la inscripción en tal libro contable.

Según González (2013), la blockchain de Bitcoin funciona como un libro contable descentralizado, en el cual los saldos no están ligados a los usuarios sino a las direcciones públicas que ellos controlan. El historial de todos los movimientos de Bitcoin permanece almacenado en la cadena de bloques, la cual es una base de datos distribuida, que mantiene el registro de todas las transacciones, en cada uno de los múltiples nodos que integran la red.

Para Tapscott, D. y Tapscott, A. (2016), la blockchain es una verdadera plataforma global abierta y distribuida, que cambiará fundamentalmente lo que podemos conseguir en línea, como lo hacemos y quién puede participar en ésta. La cadena de bloques puede contener cualquier documento legal, además de contratos inteligentes que podrían cambiar la manera en la que las empresas realizan la gestión, el funcionamiento y el pago de títulos de valores, documentos, activos digitales y hasta acuerdos entre personas.

Según Mougayar (2016), la blockchain es una tecnología del libro mayor de contabilidad descentralizada, que permite transformarse y combinar, con armonía, la ciencia criptográfica, la teoría de juegos y la ingeniería del software.

Para Santiago (2019), la blockchain es un registro contable público (libro mayor de acontecimientos digitales, cuyas transacciones pueden ser verificadas por cualquiera) y descentralizado, que contiene todas las transacciones realizadas, desde la génesis de Bitcoin y que es compartido entre todos los usuarios de Bitcoin, mediante un sistema P2P, haciendo imposible la falsificación y muy fácil la verificación. También, esta cadena de bloques previene el doble gasto, es imborrable y verifica la estabilidad de las transacciones Bitcoin, las cuales contienen la dirección Bitcoin de origen, la dirección de destino y la cuantía de la transacción.

Atendiendo a las definiciones recogidas de los expertos anteriores, entendemos Blockchain como un libro contable descentralizado, el cual contiene todos los registros que se han llevado a cabo de forma ordenada, recibiendo estos el nombre de bloques. Cada bloque tiene un hash (número de identificación del bloque), y además también contiene el hash del bloque anterior, por lo que cada bloque queda conectado con su predecesor y su sucesor. El resultado de todo esto es un libro contable que se administra de forma autónoma y de manera descentralizada. (Santiago Moreno, 2017)

4.2. PROPIEDADES DE BLOCKCHAIN

A continuación, pasamos a describir las ocho propiedades de las que consta una blockchain:

- Tokenización: los tokens digitales significan tres cosas, que la representación del valor es digital, que el control del token lo determinan las claves criptográficas y que el registro de la propiedad del token radica en la cadena de bloques. La combinación de estas tres cosas da sentido a la tokenización, donde se concentra la capacidad de innovación disruptiva de blockchain.
- Protocolo: definimos protocolo estándar como un programa informático para que una red de ordenadores (nodos) pueda comunicarse entre sí. El protocolo de una blockchain proporciona un estándar de cómo se tienen que comunicar los ordenadores participantes en la red. Como ejemplo de protocolos exitosos tenemos a Bitcoin y Ethereum, entre otros. El beneficio de la nueva estructura económica descentralizada que promete la nueva economía blockchain lo encontramos en los protocolos, los cuales serán los encargados de canalizar el internet del valor.
- Descentralización: se trata de un sistema que permite que usuarios que no confían plenamente entre ellos puedan mantener un consenso sobre la existencia, el estado y la evolución de una serie de elementos compartidos. El consenso es la clave de un sistema blockchain porque es el fundamento que permite que todos los participantes en el mismo puedan confiar en la información que se encuentra grabada en él. Este sistema basado en la confianza y el consenso se crea a partir de una red global de ordenadores que administran una enorme base de datos. Cada vez que se alcanza un consenso, una transacción se registra en un bloque, que es un espacio de almacenamiento. La cadena de bloques realiza un seguimiento de estas transacciones que pueden verificarse posteriormente como realizadas. La cadena de bloques puede estar abierta a la participación de cualquiera que lo desee (blockchain pública) o bien limitada a solo ciertos usuarios (blockchain privada), aunque siempre sin la necesidad de que exista una entidad central que supervise o valide los procesos que se lleven a cabo.
- Contabilidad pública distribuida: la tecnología de la cadena de bloques es un registro público y distribuido de transacciones, con una marca de tiempo que permite el seguimiento de dichas transacciones procesadas en su red, donde

cada usuario verifica la validez de cada una de estas, lo que evita el doble gasto. Los registros de blockchain son permanentes, se ordenan cronológicamente y están disponibles para todos los otros nodos.

- Software de código abierto: la mayoría de las cadenas de bloques son de código abierto y sus fuentes de software son públicas; en ellas, la innovación fluye de forma colaborativa.
- Red entre iguales (P2P): una red entre iguales o P2P es una red de nodos (puede ser desde un ordenador personal a una mega computadora) conectados directamente en una misma red. La base de la blockchain se construye sobre una red entre iguales (P2P) donde la computadora es la red. La comunicación siempre ocurre directamente entre pares, en lugar de a través de algún nodo central. En la cadena de bloques, la información se almacena en cada nodo y luego se pasa al nodo adyacente, propagándose así a través de toda la red.
- Criptografía: la criptografía proporciona a la cadena de bloques un mecanismo para la codificación segura de las reglas del protocolo que rigen el sistema, con lo que se evitan hurtos, manipulaciones y errores de información en la blockchain.
- Teoría de juegos: la teoría de juegos es el estudio de la toma de decisiones estratégicas. Un modelo de teoría de juegos tiene al menos tres componentes: los jugadores, que son los que toman las decisiones; las estrategias, que son las decisiones competitivas que se quieren tomar, y el resultado, que es el conjunto de consecuencias de las estrategias. En la teoría de juegos hay dos tipos de juegos:

  Juego de suma cero: juego en el que la ganancia de un jugador se obtiene a costa de otro jugador.

  Juego sin suma cero: juego donde la ganancia de un jugador no se consigue a expensas de otro jugador.

  El equilibrio de Cournot y Nash asume que cada jugador conoce y ha adoptado su mejor estrategia y que todos conocen las estrategias de los otros jugadores. Por tanto, cada jugador no gana nada modificando su estrategia si los otros no han cambiado las suyas. Formulado inicialmente por Antonie Augustin Cournot en 1838 y completado en 1951 por John Forbes Nash, este concepto tiene enormes implicaciones en el concepto de la cadena de bloques, ya que el protocolo de blockchain asume el equilibrio de Cournot y Nash. (Santiago Moreno, 2019)

4.3. TIPOS DE BLOCKCHAIN

La tecnología blockchain ha evolucionado mucho desde su aparición, una evolución que ha llamado la atención de muchos actores a nivel mundial. En los inicios de esta tecnología, los principales interesados fueron individuos con la capacidad de ver la transformación y la revolución que traería. Una tecnología pública y al alcance de todos, tanto para mejorarla como para participar activamente en la misma. Pasó algún tiempo hasta que las empresas y los gobiernos pusieran interés en la tecnología para usarla en sus propios proyectos.

Pero los intereses de las empresas y gobiernos son distintos a los de las comunidades abiertas. Esta visión dio como origen el nacimiento de proyectos blockchain distintos a

todo lo conocido. Fue así como nacieron las blockchain privadas y las blockchain híbridas o federadas. (*Bit2me.Com*)

- Blockchain Pública: Una blockchain pública es una red descentralizada de ordenadores que utilizan un protocolo común empleado por todos los usuarios y que les permite registrar transacciones en el libro mayor de la base de datos. Estas anotaciones son incorruptibles e inalterables, si bien los usuarios de una blockchain de estas características pueden validar por consenso y de forma independiente los cambios que se realizan en los registros. Ethereum y Bitcoin son ejemplos de cadenas de bloques públicas (Santiago Moreno, 2019). Entre las características de las blockchain públicas podemos mencionar:

- *Permiten que cualquier persona pueda formar parte de la misma*. Bien sea como usuario, minero o administrador de un nodo, las personas pueden acceder a la red y formar parte de ella sin restricción alguna.
- *El funcionamiento de la red es completamente transparente y abierto***.** Los datos de la blockchain desde sus inicios están disponibles para todos sin restricciones. Cualquier persona puede revisar o auditar el funcionamiento de la red y su software.
- *No existen entidades centralizadas***.** Las redes públicas son completamente descentralizadas y no existe una autoridad central que regule su funcionamiento.
- *El mantenimiento económico de la blockchain depende del sistema integrado en la misma.* Generalmente este sistema económico depende de la minería y el cobro de comisiones por cada transacción que se realice dentro de la red. (*Bit2me.Com*)

- Blockchain privada: Las cadenas de bloques privadas son aquellas en las que el proceso de consenso y la participación está limitado y en las que los permisos de escritura se mantienen centralizados en una sola organización. Además, la lectura de la información registrada en la cadena de bloques puede también estar limitada a determinados participantes (Santiago Moreno, 2017).Por ejemplo, uno de los argumentos esgrimidos por el sector financiero y otros sectores regulados para el desarrollo de las blockchains privadas ha sido la imposibilidad de compartir, por razones regulatorias o de confidencialidad, sus bases de datos abiertas. R3 y Digital Assets Holdings son ejemplos de cadenas de bloques privadas (Santiago Moreno, 2019). Entre las características de este tipo de redes podemos mencionar:

- *El acceso a la red está restringido a elementos que solo pueden ser autorizados por la unidad central de control.*
- *El acceso al libro de transacciones o cualquier otro medio de información generado por la blockchain es privado*.
- *El mantenimiento económico de la blockchain depende generalmente de la empresa que sostenga el proyecto*. Con frecuencia, las blockchain privadas no cuenta con criptomonedas ni se realizan acciones de minería.

- Blockchain híbrida o federada: Este tipo de blockchain es una fusión entre las blockchain públicas y las privadas. Es un intento de aprovechar lo mejor de ambos mundos. En estas blockchain, la participación en la red es privada. Es decir, el acceso a los recursos de la red es controlado por una o varias entidades. Sin embargo, el libro de contabilidad es accesible de forma pública. Esto significa que cualquier persona puede explorar bloque a bloque todo lo que sucede en dicha blockchain.

Por ejemplo, este tipo de redes blockchain son muy útiles para gobiernos u organizaciones empresariales que deseen almacenar o compartir datos de forma segura. Un perfecto caso de uso está sucediendo en el sector sanitario, donde se empieza a usar blockchain para almacenar los datos de sus líneas de producción de medicamentos. Los datos almacenados pueden ser revisados por la autoridad competentes con el fin de controlar la calidad, tanto a nivel de la misma empresa como de gobierno. El objetivo de la aplicación de este modelo de blockchain es mantener un alto de nivel de transparencia y confianza. Entre las características de este tipo de redes podemos mencionar:

- *El acceso a la red está restringido a elementos que solo pueden ser autorizados por el resto de las unidades de control.*
- *El acceso al libro de transacciones o cualquier otro medio de información generado por la blockchain es público.*
- *No existe minería ni criptomonedas.* El consenso de la red se da por otros medios que aseguran que los datos son correctos.
- *Es parcialmente descentralizado lo que conlleva a un mejor nivel de seguridad y transparencia.* (*Bit2me.Com*)

CAPÍTULO 5: ¿QUÉ ES LA NUEVA ECONOMÍA BLOCKCHAIN?

La nueva economía blockchain es una continuación evolucionada de lo que llegó a definirse como nueva economía. La nueva economía blockchain es la siguiente fase de la evolución de internet a la que denominamos << la era de la descentralización>>, en donde blockchain juega un papel clave. El término nueva economía fue acuñado por el economista Brian Arthur y popularizado por Kevin Kelly, editor de la revista Wired. Este término fue ideado a finales de los años noventa para describir la evolución de una economía basada principalmente en la producción industrial a otra basada en el conocimiento, debido a los nuevos progresos en tecnología y a la globalización económica. Para algunos analistas este cambio de estructura económica había creado un estado de crecimiento constante y permanente, de desempleo bajo y relativamente inmune a los ciclos macroeconómicos. La base de la nueva economía estaba en un crecimiento sin inflación, con fuertes aumentos de productividad, donde internet era el sistema de organización de la nueva economía.

La descentralización impulsa el capitalismo, abriendo oportunidades de nuevos modelos de negocio y creando nuevas capas de producción, colaboración, trabajo y creación de valor, en general.

Para entender la nueva economía, hay que conocer los principios y las leyes en las que esta se basa:

- Principio de la abundancia.

La abundancia rige una economía interconectada. En la economía interconectada, cuanto más abundante son las cosas, más valor obtenemos. El principio de la abundancia se expresa de una forma más precisa del siguiente modo: en una red, cuantas más oportunidades se aprovechen, más rápido aparecerán oportunidades nuevas.

Tradicionalmente en la economía, el valor procede de la escasez: oro, diamantes, Ferraris, etc. Pero la lógica de la red da un giro a todo esto haciendo que, en la

economía interconectada, el valor proceda de la abundancia. Las relaciones se disparan en valor a medida que se incrementan las partes implicadas.

- Ley de Moore.

En 1965, Gordon Moore, cofundador de Intel, afirmó que, aproximadamente cada dos años se duplica el número de transistores en un microprocesador. La consecuencia directa de esta ley es que los precios bajan, a la vez que las prestaciones aumentan. Esta ley también afecta al equipamiento informático que se emplea en la minería de la cadena bloques.

- Ley de Metcalfe

A medida que el número de intervinientes de una red aumenta aritméticamente, el valor de la red aumenta exponencialmente. La incorporación de unos cuantos miembros puede incrementar drásticamente el valor para todos los miembros. Cuando el número de individuos (n) involucrados es grande, el número total de conexiones se puede estimar de una forma sencilla como n^2. La magia de n^2 es que, cuando se incorpora un nuevo miembro está incorporando además muchas más conexiones y más valor. En el mundo industrial esto no es así. Supongamos que Mirella fuera propietaria de una panadería y que tuviera diez clientes que compran pan diariamente. Si aumentase su cartera de clientes en un 10% incorporando un nuevo cliente, podríamos esperar un aumento de las ventas de un 10%, es decir, un incremento lineal. Pero supongamos, en cambio, que fuera propietaria de una red social formada por diez usuarios que se comunicarán una vez entre sí al día. Sus usuarios harían unas n^2 o cien comunicaciones diarias. Si incorporase un nuevo usuario más, aumentaría su base de clientes en un 10%, pero las posibilidades de negocio aumentarían en mayor medida.

La tendencia de la red de incrementar su valor matemáticamente fue anunciada por primera vez por Bob Metcalfe, inventor de una tecnología de redes denominada Ethernet.

- Ley de rendimientos crecientes.

El valor de una red se dispara a medida que aumenta el número de sus miembros. Esto quiere decir que las redes contribuyen a que los que tienen éxito todavía tengan más éxito. El economista Brian Arthur denomina a este efecto rendimientos crecientes y estos suponen una tendencia a que lo que va por delante vaya todavía más por delante y que lo que se queda atrás se vaya quedando cada vez más atrás. En la economía industrial, el éxito es autolimitador, ya que obedece a la ley de los rendimientos decrecientes, donde el valor se incrementa linealmente: pequeñas acciones generan pequeños resultados, y las grandes acciones generan grandes resultados. En cambio, en la economía interconectada, el éxito es autorreforzador y obedece a la ley de los rendimientos crecientes, por lo que las pequeñas acciones se refuerzan entre sí de modo que los resultados pueden crecer rápida y exponencialmente. Los rendimientos crecientes son generados y compartidos por toda la red.

Blockchain permite un nuevo flujo de valor que transforma las cadenas de suministros globales debido a que generan una aceleración en el flujo de conocimiento, de la tecnología y del aprendizaje que termina traduciéndose en un mayor crecimiento en la economía.

Mientras que internet supuso una transformación sin precedentes en el acceso e intercambio de información, la cadena de bloques lo será en el intercambio de activos, llevándonos al denominado internet del valor. Este encuentra su base en la tecnología blockchain. De la misma forma que podemos acceder a páginas web en todo el mundo en el internet de la información, en el internet del valor tenemos una

herramienta nueva para compartir y gestionar bienes digitales, sin la necesidad de depender de una entidad que centralice el proceso, gracias a la tokenización y a la labor que desempeñará la criptografía. (Santiago Moreno, 2019)

CAPÍTULO 6: FINANZAS DESCENTRALIZADAS O DEFI

DeFi es el acrónimo del término Finanzas descentralizadas y actualmente es uno de los sectores de más rápido crecimiento en el espacio blockchain y criptomonedas.

El nacimiento de DeFi como lo conocemos comenzó en la blockchain de Ethereum. La capacidad de Ethereum para ofrecer smart contracts flexibles, fue lo que hizo posible este paso. Para 2018, Ethereum tenía ya en activo unos 15 proyectos dedicados a DeFi. Sobre todo, proyectos dedicados a mercados de liquidez, sistemas de préstamos y Exchanges descentralizados (DEX). Los cuales abordaremos en los capítulos posteriores. (*Cointelegraph.Com*)

DeFi busca construir un mejor panorama financiero hecho posible gracias a la llega de internet y la tecnología blockchain, particularmente en los siguientes aspectos:

- *Accesibilidad*: Las finanzas descentralizadas amenazan con eliminar gradualmente las finanzas tradicionales debido a su capacidad para proporcionar servicios financieros sin barreras geográficas. Las finanzas tradicionales han luchado por llegar a algunas partes remotas del mundo, dejando a miles de millones sin acceso a los servicios bancarios.

  El Banco Mundial estima que en 2017 había 1700 millones de personas que no poseían una cuenta en una institución financiera y más de la mitad de ellas son de países en desarrollo. Mientras que estima que dos tercios de los 1700 millones de personas tienen acceso a los teléfonos móviles. (Lau et al., 2020)

  De esta forma, gracias a la integración de tecnologías de contabilidad digital en aplicaciones, las personas en lugares remotos del mundo ahora pueden acceder a los servicios bancarios a través de sus dispositivos móviles y acceso a internet.

- *Abordar los problemas financieros mundiales*: Después de la crisis financiera de 2008, muchas personas perdieron su fortuna debido a la quiebra de un buen número de bancos. Preocupados por la amenaza que representan los sistemas financieros globales actuales, muchas personas están buscando tecnologías emergentes para protegerse.

  Las finanzas descentralizadas también están demostrando ser un método confiable para eludir problemas relacionados con la hiperinflación resultante de la manipulación de la moneda o devaluaciones inesperadas, como es el caso de China.

- *Eludir la censura y las restricciones*: Las finanzas descentralizadas podrían hacer posible que la gente eluda las prohibiciones o restricciones impuestas por gobiernos opresores. El sector financiero tradicional viene con una gran cantidad de regulaciones y requisitos que, a veces, dificultan que las personas que cruzan las fronteras realicen transacciones comerciales.

  La integración de la tecnología blockchain en una serie de productos financieros, hace posible que las personas envíen y reciban dinero sin tener que preocuparse por prohibiciones o restricciones. El hecho de que las personas no puedan rastrear transacciones con el uso de tecnologías de contabilidad digital

hace posible completar transacciones sin tener que preocuparse por violaciones de privacidad por parte de los gobiernos.

La capacidad de proporcionar acceso sin censura a los servicios financieros globales es una de las razones por las que las finanzas descentralizadas seguirán destacando de las finanzas tradicionales. En un mundo donde las personas valoran su privacidad, cualquier producto que permita evitar las usurpaciones no éticas de la privacidad por parte de las autoridades será exitoso.

- *Mejorar los sistemas de pagos*: las criptomonedas que impulsan el movimiento DeFi buscan eludir a los intermediarios financieros, realizar transferencias de manera más rápida, sin preguntas y con comisiones relativamente más bajas en comparación con las que cobran los bancos.

  De esta forma las finanzas descentralizadas aportan una solución a la problemática que nos ofrecen las finanzas centralizadas si queremos enviar dinero a alguien o a una empresa en otro país. (*Medium.Com*)

6.1. ¿QUÉ ES DEFI?

Finanzas descentralizadas o DeFi es el movimiento que permite a los usuarios utilizar servicios financieros, sin la necesidad de depender de entidades centralizadas. (Lau et al., 2020). Estos servicios financieros se llevan a cabo gracias a la unión de los smart contracts, los cuales tienen la capacidad de manejar dinero de forma autónoma y las Dapps que permiten interactuar con dicho smart contract de forma sencilla. Todo ello ejecutándose sobre la blockchain de Ethereum, donde cada acción queda grabada de forma permanente e inalterable. (*Cointelegraph.Com*)

DeFi no es un solo producto o empresa, sino que es un conjunto de productos o servicios que actúa como un reemplazo de las instituciones, que van desde la banca, seguros, bonos y mercados monetarios.

Para que DeFi Dapps funcione, por lo general requiere que la garantía se bloquee en contratos inteligentes. La garantía acumulada bloqueada en DeFi Dapps se conoce a menudo como el valor total bloqueado. Según DeFi Pulse, el valor total bloqueado a principios de 2019 midió alrededor de 275 millones de dólares, pero en abril de 2021, alcanzó un máximo de 62,000 millones de dólares. El gran crecimiento del valor total bloqueado sirve como indicador del rápido crecimiento del ecosistema DeFi. (Lau et al., 2020)

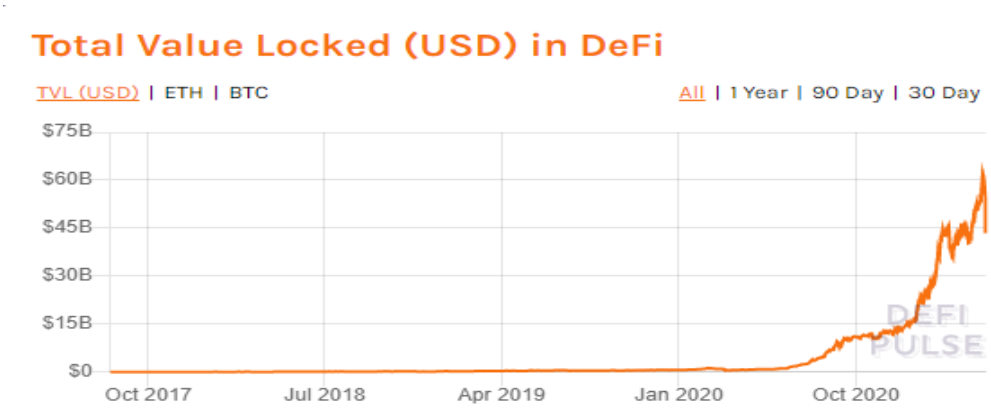

Figura 6.5. Valor total bloqueado en DeFi

Fuente: (*Defipulse.Com*)

6.2. ¿QUÉ TAN DESCENTRALIZADO ES DEFI?

El grado de descentralización varía según cada protocolo, activo y aplicación, e incluso las cosas que están descentralizadas pueden adquirir una forma centralizada a través de intercambio de custodia y otros agregadores.

Los componentes comunes entre todos los protocolos de préstamos DeFi incluyen custodia, precios, inicio de llamadas de margen, provisión de liquidez de llamadas de margen, determinación de la tasa de interés y desarrollo de protocolos. Estos componentes nos ayudan a determinar el grado de control que los equipos detrás de los protocolos tienen sobre los activos retenidos.

Las diferentes categorías según su grado de descentralización son las siguientes:

- *CeFi*: Los productos CeFi son de custodia, utilizan alimentadores de precios centralizados, inician llamadas de margen de forma centralizada, determinan de forma centralizada las tasas de interés y proporcionan liquidez de forma centralizada para sus llamadas de margen.
- *DeFi de grado 1*: estos productos DeFi no son de custodia, pero utilizan alimentadores de precios centralizados, inician llamadas de margen de forma centralizada, proporcionan liquidez de forma centralizada, determinan de forma centralizada las tasas de interés y administran de forma centralizada los desarrollos y actualizaciones de la plataforma.
- *DeFi de grado 2*: estos productos DeFi no son de custodia y tienen un componente descentralizado adicional que podría incluir alimentación de precios, inicio de llamadas de margen, liquidez de margen, determinación de la tasa de interés o desarrollo de la plataforma, mientras que el resto aún está centralizado.
- *DeFi de grado 3*: estos productos DeFi no son de custodia, tienen el inicio sin permiso de las llamadas de margen y la provisión sin permiso de liquidez de las llamadas de margen, mientras administran de manera centralizada las alimentaciones de precios, controlan de manera centralizada las tasas de interés, los desarrollos y actualizaciones de la plataforma.
- *Grado 4 DeFi*: estos productos DeFi no son de custodia, tienen llamadas de margen sin permiso, provisión sin permiso de liquidez de llamadas de margen y alimentaciones de precios descentralizadas, pero determinan de manera centralizada las tasas de interés y controlan de forma centralizada los desarrollos y actualizaciones de la plataforma.
- *Grado 5 DeFi*: estos productos DeFi no son de custodia, tienen llamadas de margen sin permiso, provisión sin permiso de liquidez de llamadas de margen, alimentaciones de precios descentralizadas y determinación de la tasa de interés descentralizada, pero controlan de forma centralizada los desarrollos y actualizaciones de la plataforma.
- *Grado 6 DeFi*: todos los componentes de estos protocolos DeFi, incluido el desarrollo, están descentralizados. No hay ejemplos existentes, ya que ningún protocolo DeFi está completamente descentralizado. (*Hackernoon.Com*)

CAPÍTULO 7: LAS STABLECOINS

Los precios de las criptomonedas son extremadamente volátiles. Para mitigar esta volatilidad, se crearon las stablecoins. Este nuevo tipo de criptomonedas son tokens que están asociados al valor de una moneda “Fiat” (como el dólar o el euro), a bienes materiales como el oro o los inmuebles, o a otra criptomoneda. En este capítulo nos centraremos en el token cuyo valor está respaldado por una moneda “Fiat” por medio de Tether y en el token donde su valor está asociado a otra criptomoneda a través de DAI. (*Bbva.Com*)

7.1. TETHER (USDT)

Tether (USDT) es la primera stablecoin del mundo (una criptomoneda que reproduce el valor de una moneda fíat). Originalmente, se lanzaría en 2014 bajo el nombre "Realcoin", por el inversor de Bitcoin Brock Pierce, el emprendedor Reeve Collins y el desarrollador de software Craig Sellers. (*Binance.Com*)

Realcoin sería inicialmente emitida en el protocolo bitcoin a través de Omni Layer. Con el uso de Omni Layer, Pierce y Sellars pudieron lanzar a Realcoin usando la blockchain de Bitcoin. Esto era posible porque Omni Layer, permite realizar operaciones con representaciones de activos. Esto significa que se puede generar, enviar, intercambiar, canjear, pagar dividendos y hacer apuestas con tokens que representan cualquier tipo de activo. Todo ello funcionando sobre una segunda capa construida sobre Bitcoin y operada directamente por el protocolo Omni.

La aparición de Realcoin sería uno de los mayores proyectos realizados sobre Omni en esos momentos. Sin embargo, más tarde Realcoin cambiaría su nombre. El 20 de noviembre de 2014, el CEO de Tether, Reeve Collins, anunció que el proyecto pasaría a denominarse Tether. (*Bit2me.Com*)

Pese a ser emitida en el protocolo Bitcoin, USDT posteriormente también migraría a otras blockchains. De hecho, como podemos observar en el gráfico que se muestra a continuación, la mayor parte de su masa monetaria se encuentra en Ethereum en forma de tokens ERC-20. También se emite en otras blockchains, entre las que figuran TRON, EOS, Algorand, Solana y OMG Network. (*Binance.Com*)

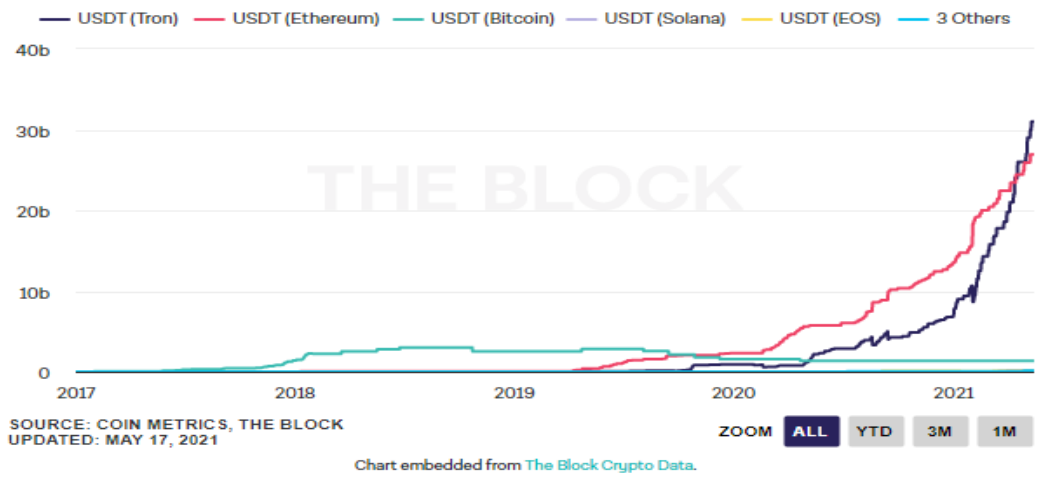

Figura 7.6. Suministro de USDT por Blockchain

Fuente: (*Binance.Com*)

7.1.1. Características técnicas de USDT

USDT es una criptomoneda bastante particular técnicamente hablando. En primer lugar, su funcionamiento es dirigido y orquestado sobre el protocolo Omni. Este protocolo se ejecuta de forma incrustada sobre una blockchain. Como resultado de esto, esta criptomoneda hereda las propiedades de los tokens de dicha blockchain y se beneficia de las capacidades que ofrece dicha blockchain.

Por otra parte, el protocolo Omni puede conceder (crear) y revocar (destruir) tokens digitales representados como metadatos integrados en la cadena de bloques. Además, permite a los usuarios realizar transacciones y almacenar enlaces y otros activos. Todo ello significa, que los tokens USDT no pueden minarse y solo se crean de acuerdo a las necesidades del ecosistema por parte de Tether.

El registro de transacciones de USDT es público y también existe la web de transparencia. Todo esto con la finalidad de ofrecer tranquilidad a la comunidad que hace uso de esta stablecoin. Esto ha llevado a la creación de la llamada Prueba de Reservas. Este sistema une la contabilidad blockchain junto a la contabilidad de sus cuentas bancarias para llevar a lo que se conoce como, Equivalencia Tether. Esta equivalencia es la que permite asegurar la relación 1:1 de colateralización.

7.1.2. Flujo de dinero y tokens en USDT

Una de las principales características técnicas de USDT viene dada por la forma en cómo se maneja el flujo de dinero entre tokens y monedas Fiat. Este es un proceso que a grandes rasgos puede dividirse en cinco etapas. Estas etapas tienen una funcionalidad específica y son las siguientes:

1. En primer lugar, el usuario deposita una determinada cantidad de dólares en la cuenta bancaria de la compañía Tether Limited.
2. Seguidamente, Tether Limited genera y acredita los tokens USDT en la cuenta del usuario. Estos son creados en una relación 1:1 con respecto al depósito realizado.
3. A continuación, ya con los fondos USDT activos, el usuario puede usarlos como cualquier criptomoneda.
4. Para que el usuario pueda cambiar sus tokens USDT, debe depositar los mismos en las cuentas de Tether Limited para canjearlos por dólares.
5. Finalmente, Tether Limited destruye los tokens USDT y envía moneda fiduciaria a la cuenta bancaria del usuario. Los usuarios también pueden obtener otras divisas o criptomonedas usando otros medios de intercambios. (*Bit2me.Com*)

7.2. DAI

Dai Stablecoin es una criptomoneda respaldada por garantías cuyo valor es estable en relación con el dólar estadounidense.

El valor de Dai se respalda y estabiliza a través de un sistema dinámico de Posiciones de deuda garantizada (CDP), mecanismos de retroalimentación autónoma y actores externos debidamente incentivados. Todo esto es posible gracias a Maker una plataforma de contrato inteligente en Ethereum.

Dai es generado por los usuarios al depositar activos colaterales en las Maker Vaults dentro del protocolo Maker. De esta forma Dai entra en circulación y los usuarios logran acceso a la liquidez.

Una vez generada, comprada o recibida, Dai puede usarse de la misma manera que cualquier otra criptomoneda: se puede enviar a otras personas, se puede usar como forma de pago de bienes o servicios, e incluso se puede guardar como ahorro mediante una función del Protocolo Maker llamada Tasa de Interés de Dai (DSR).

Cada Dai en circulación está respaldado directamente por el exceso de colateral; esto significa que el valor del colateral es mayor al de la deuda en Dai y todas las transacciones en Dai pueden verse públicamente en la cadena de bloques Ethereum.

7.2.1. Proceso de posición de deuda garantizada (CDP)

Cualquiera que tenga activos que sean aceptados como garantía, puede usarlos para generar dais en la Plataforma Maker a través de los contratos inteligentes exclusivos de Maker conocidos como Posiciones de deuda garantizada.

Los CDP tienen activos afectados con garantía depositados por un usuario y le permiten a este usuario generar dais, aunque esta actividad también genera deuda. Esta deuda bloquea efectivamente los activos afectados con garantía depositados dentro del CDP hasta que posteriormente se cubra mediante el reembolso de una cantidad equivalente de dais, en cuyo momento el propietario puede retirar nuevamente su garantía. Los CDP activos siempre están garantizados en exceso, lo que significa que el valor de la garantía es más alto que el valor de la deuda.

El proceso de interacción de CDP se lleva a cabo de la siguiente forma:

- *Paso 1. Creación de CDP y depósito de la garantía*: El usuario de CDP primero envía una transacción a Maker para crear la CDP y, a continuación, envía otra transacción para financiarla con la cantidad y el tipo de garantía que se utilizará para generar dais. En este punto, la CDP se considera garantizada.
- *Paso 2. Generar dais a partir de la CDP garantizada*: A continuación, el usuario de CDP envía una transacción para recuperar la cantidad de dais que desea a partir de la CDP y, a cambio, la CDP acumula una cantidad equivalente de deuda, lo que bloquea el acceso a la garantía hasta que se pague la deuda pendiente.
- *Paso 3. Pagar la deuda y la tarifa de estabilidad*: Cuando el usuario desea recuperar su garantía, tiene que pagar la deuda en la CDP, más la tarifa de estabilidad que se acumula continuamente sobre la deuda a lo largo del tiempo. La tarifa de estabilidad solo se puede pagar en MKR. Una vez que el usuario envía el requisito de dais y MKR a la CDP, paga la deuda y la tarifa de estabilidad, la CDP queda libre de deudas.
- *Paso 4. Retirada de la garantía y cierre de la CDP*: Con la deuda y la tarifa de estabilidad pagadas, el usuario de CDP puede recuperar de manera gratuita todas o algunas de sus garantías en su billetera enviando una transacción a Maker.

Para comprender mejor el proceso CDP, a continuación, se muestra un ejemplo de dicha operativa:

Manuel necesita un préstamo, por lo que decide generar 100 dais. Bloquea una cantidad de ETH que vale mucho más de 100 dais en un CDP y la usa para generar 100 dais. Los 100 dais se envían instantánea y directamente a su cuenta Ethereum. Suponiendo que la tarifa de estabilidad sea de 1% al año, Manuel necesitará 101 dais

para cubrir el CDP si decide recuperar su ETH un año después. La tarifa de estabilidad se denomina en Dais, pero solo se puede pagar utilizando el token MKR.

7.2.2. Mecanismos de estabilidad de precios

El precio objetivo del Dai tiene dos funciones principales en la plataforma Maker: 1) Se utiliza para calcular la relación entre la garantía y la deuda de una CDP, y 2) Se utiliza para determinar el valor de los activos afectados con garantía que los titulares de dais reciben en el caso de una liquidación global.

El precio objetivo se denomina inicialmente en USD y comienza en 1, lo cual se traduce en una paridad fija de 1:1 USD.

Para garantizar que siempre haya una garantía suficiente en el sistema para cubrir el valor de toda la deuda pendiente (según el precio objetivo), puede liquidarse un CDP si se considera que su nivel de riesgo es excesivo. La plataforma Maker determina cuándo liquidar un CDP comparando la proporción de liquidación con la proporción actual entre la garantía y la deuda del CDP.

Cada tipo de CDP tiene su propia proporción de liquidación que está controlada por los votantes de MKR y se establece en función del perfil de riesgo del particular activo de la garantía de ese tipo de CDP.

El proceso de liquidación se lleva a cabo mediante un mecanismo de subasta de deudas y garantías, el cual tiene el siguiente funcionamiento:

Durante una liquidación, la plataforma Maker compra la garantía de un CDP y posteriormente la vende en una subasta automática. Este mecanismo de subasta permite que el sistema liquide CDP incluso cuando no hay disponible información sobre los precios.

Con el fin de tomar posesión de la garantía del CDP para poder venderla, el sistema primero necesita recaudar suficientes dais para cubrir la deuda del CDP. Esto se llama subasta de deuda, y consiste en diluir el suministro de tokens MKR y venderlo a los licitantes en un formato de subasta.

Paralelamente, la garantía del CDP se vende en una subasta de garantías en la cual todos los ingresos (también denominados en dais) hasta la cantidad de deuda CDP más una penalización por liquidación (un parámetro de riesgo determinado por votación MKR) se utiliza para comprar MKR y eliminarlo del suministro. Esto contrarresta directamente la dilución de MKR que se produjo durante la subasta de deuda. Si se ofertan suficientes dais para cubrir completamente la deuda de CDP más la penalización por liquidación, la subasta de garantías cambia a un mecanismo de subasta inversa e intenta vender la menor cantidad de garantías posible: cualquier garantía sobrante se devuelve al titular original del CDP.

Para comprender mejor este proceso, a continuación, se muestra un ejemplo:

Supongamos que hay un tipo Ether CDP con una proporción de liquidación del 145%, una proporción de penalización del 105%, y tenemos un Ether CDP con una proporción entre la garantía y la deuda del 150%. El precio del Ether ahora cae al 10% frente al precio objetivo, lo que hace que la proporción entre la garantía y la deuda del CDP caiga al ~135%. Puesto que está por debajo de la proporción de liquidación, los operadores pueden desencadenar su liquidación y comenzar a pujar con dais para comprar MKR en la subasta de deuda. Simultáneamente, los corredores de bolsa pueden comenzar a pujar con dais para comprar la garantía por valor de 135 dais en la subasta de garantías. Una vez que se ofertan al menos 105 dais sobre la garantía de Ether, los corredores de bolsa invierten la oferta para obtener la menor cantidad de garantía por 105 dais. Cualquier garantía restante se devuelve al propietario de CDP.

En caso de que ocurrieran emergencias serias con un comportamiento irracional del mercado a largo plazo, piratería o infracciones de seguridad y actualizaciones del sistema se activaría la liquidación global, la cual es un proceso que puede utilizarse como último recurso para garantizar criptográficamente el precio objetivo a los titulares de Dais. Desactiva y cierra progresivamente la plataforma Maker al tiempo que garantiza que todos los usuarios, tanto los titulares de Dais como los usuarios de CDP, reciban el valor neto de los activos a los que tienen derecho. El proceso está completamente descentralizado y los votantes de MKR gobiernan el acceso al mismo para garantizar que solo se use en caso de emergencias graves.

El proceso de liquidación global se llevaría a cabo de la siguiente manera:

- *Paso 1. Se activa la liquidación global*: Si hay suficientes actores designados como liquidadores globales por el cuerpo rector de Maker que creen que el sistema ha sido sometido a un ataque grave, o si se ha programado una liquidación global como parte de una actualización técnica, pueden activar la función de liquidación global. Esto detiene la creación y manipulación de CDP, y congela el índice de precios en un valor fijo que luego se utiliza para procesar las reclamaciones proporcionales para todos los usuarios.
- *Paso 2. Se procesan las reclamaciones de liquidación global*: Después de que se haya activado la liquidación global, se necesita un período de tiempo para permitir que los guardabarreras procesen las reclamaciones proporcionales de todos los titulares de dais y CDP en función del valor de índice fijo. Una vez finalizado este procesamiento, todos los titulares de dais y titulares de CDP podrán reclamar una cantidad fija de ETH con sus dais y CDP.
- *Paso 3. Los titulares de dais y de CDP reclaman la garantía con sus dais y CDP*: Cada titular de dais y de CDP puede presentar una función de reclamación en la plataforma Maker para intercambiar sus dais y CDP directamente por un monto fijo de ETH que corresponde al valor calculado de sus activos, en base al precio objetivo del Dai. (Dai-Whitepaper, 2017)

CAPÍTULO 8: PROTOCOLOS LÍDERES EN EL MERCADO DEFI

Una vez que conocemos que es DeFi y cuál es el funcionamiento que hay detrás de toda esta tecnología, pasamos a ver los principales protocolos líderes en el mercado DeFi.

8.1. NEXUS MUTUAL

Nexus Mutual es un protocolo de seguro descentralizado basado en Ethereum. Se constituye como una sociedad limitada por garantía en el reino unido y opera bajo una estructura de mutua discrecional, es decir, todas las reclamaciones de seguro se pagan a potestad de la junta (los miembros de Nexus Mutual).

Actualmente Nexus Mutual ofrece cobertura contra fallos de contrato inteligente. La cobertura que ofrece Nexus Mutual proporciona protección contra pérdidas financieras que pueden ser incurridas debido a hacks o exploits en el código del contrato inteligente. La pérdida de claves privadas o los hacks de intercambio centralizado, no se encuentran dentro de la cobertura que ofrece dicha aseguradora. (Lau et al., 2020)

La cobertura de este seguro se lleva a cabo a través de su token nativo, NXM, así como también se utiliza para participar en el ecosistema a través de la evaluación de

reclamos, la evaluación de riesgos y la gobernanza. Además, los tokens representan derechos de membresía y un reclamo sobre el capital de la mutua.

El precio del token se determina, a través de un modelo de token continuo, también conocido como curva de balance. El precio del token está instigado por dos factores principales: el monto del capital requerido para respalda las coberturas escritas (MCR) y el nivel de financiación de la mutua con respecto al capital mínimo obligatorio (% MCR).

El capital mínimo (MCR) representa la cantidad mínima de fondos necesarios para pagar todas las reclamaciones con un 99,5% de confianza. El MCR se estableció en el lanzamiento por 7,000 ETH y aumenta gradualmente cuando se compran más cubiertas. Siempre que el MCR esté por encima del nivel mínimo, el precio del token aumentará a medida que se compren nuevas cubiertas y disminuirá cuando vencen las cubiertas.

El otro factor decisivo del precio es el % MCR, que se puede considerar como el índice de sobre garantía de la mutua, el cual se determina por la cantidad total de fondos en el fondo común de capital en relación con el MCR. En el modelo de token, MCR% es uno de los impulsores de precios a corto plazo, mientras que MCR es un indicador de crecimiento a largo plazo y uso tangible de la plataforma.

El precio del token se calcula de la siguiente manera:

$$Precio=A+(MCRETH/C) * MCR\%^{4}$$

- Precio= Precio del token en Ether.
- MCRETH: Cantidad mínima de capital para respaldar las coberturas existentes en Ether. El requisito de capital mínimo (MCR) esta calibrado a un nivel de solvencia del 99,5%.
- MCR%: Relación de los fondos comunes de capital con respecto al MCR.
- A: Constante fija, que se calibra en función del precio de Ether vigente en el momento de lanzamiento.
- C: Constante fija, que se calibra en función del precio de Ether vigente en el momento de lanzamiento. (*Substack.Com*)

La mutua dispondrá de fondos adecuados cuando la cantidad de dinero que posee (capital pool) es mayor que el MCR. Por otro lado, el MCR% impacta directamente en el precio del token. El precio del token aumenta cuando la mutua tiene fondos adecuados. Esto lo podemos apreciar en la siguiente gráfica:

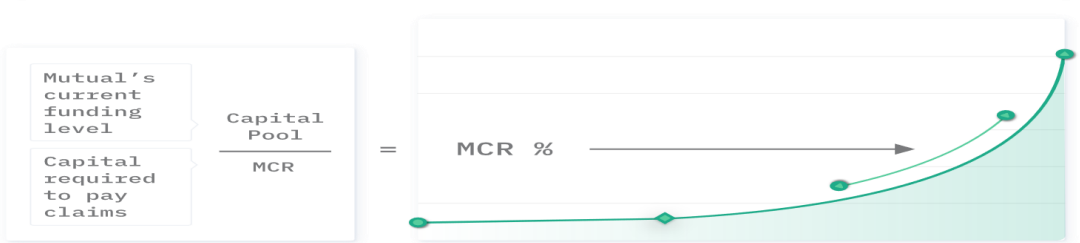

Figura 8.7. Aumento del precio del token

Fuente: (*Nexusmutual.Io*)

Cuando el capital pool disminuye, también lo hace el precio del token. Por ejemplo, cuando se paga un reclamo, el capital pool se reduce, pero el MCR permanece casi

sin cambios, lo que significa que el % de MCR disminuye, lo que reduce el precio del token. Lo podemos observar a través de la siguiente gráfica:

Figura 8.8. Disminución del precio del token

Fuente: (*Nexusmutual.Io*)

En caso de que se compre cobertura, aumenta el tamaño del fondo de capital, el MCR también aumenta, pero en casi todos los casos menos que el capital pool. Por tanto, MCR% aumenta, elevando el precio del token.

Figura 8.9. Aumento del MCR% en relación con el precio del token

Fuente: (*Nexusmutual.Io*)

Cada vez que se compra cobertura aumenta el requisito de capital mínimo (en Ether) en una pequeña cantidad si el MCR está por encima de un nivel mínimo, el cual se estable en el lanzamiento.

La mayoría de los movimientos de precios a corto plazo serán estimulados por cambios de MCR %, el crecimiento de MRCETH en las compras de cobertura será un impulsor del precio a largo plazo, lo que refleja la adopción de la plataforma. (*Nexusmutual.Io*)

Como Nexus Mutual utiliza una curva de vinculación, la emisión de nuevos tokens se produce cuando se aporta capital a la mutua o mediante recompensas por participar en el ecosistema. La emisión de token de NXM se puede dividir en las siguientes áreas:

- Tokens iniciales, los cuales están reservados para los fundadores y los primeros contribuyentes cuando se implantó el contrato.
- Comprando a través del modelo de precio token, creado cuando se compra a través de la curva de vinculación.
- Recompensas por evaluación de reclamaciones, asignado como incentivo para realizar la evaluación de reclamaciones.
- Recompensa por evaluación de riesgos, asignado como incentivo para realizar la evaluación de riesgos.
- Gobernanza, asignado como incentivo para participar en la gobernanza.

Cabe destacar que solo los miembros de Nexus Mutual pueden comprar, mantener y usar NXM. (*Substack.Com*)

8.2. MAKER_DAO

MakerDAO es un proyecto de código abierto basado en la cadena de bloques de Ethereum y una organización descentralizada autónoma creada en 2015. El proyecto es gestionado por personas de todo el mundo que tienen su token de gobernanza, MKR. Mediante un sistema de gobernanza científica, que incluye, por un lado, encuestas de gobernanza, la cual se lleva a cabo para establecer un consenso aproximado en cuanto a la opinión de la comunidad antes de que se emita un voto ejecutivo y, por otro lado, las votaciones ejecutivas, que se lleva a cabo para aprobar (o no) los cambios en el estado del sistema. Los tenedores de MKR son los encargados de gestionar el protocolo de Maker y los riesgos financieros de Dai para garantizar su estabilidad, transparencia y eficiencia. El peso de MKR en la votación es proporcional a la cantidad de MKR con los que participa un votante en el contrato de votación. Por tanto, mientras más tokens de MKR estén bloqueados en el contrato, mayor será el poder de decisión del votante.

Los tenedores de MKR pueden votar para lo siguiente:

- Agregar un nuevo tipo de activo colateral con un conjunto único de parámetros de riesgo.
- Cambiar los parámetros de riesgo de uno o más tipos de activos colaterales existentes, o añadir nuevos parámetros de riesgo a uno o más tipos de activos colaterales existentes.
- Modificar la Tasa de Interés de Dai.
- Elegir el conjunto de fuentes de oráculos.
- Elegir el conjunto de oráculos de emergencia.
- Activar el apagado de emergencia.
- Actualizar el sistema.

Por otro lado, el Protocolo Maker, construido a partir de la cadena de bloques de Ethereum, permite que los usuarios puedan crear Dai. Los elementos que actualmente integran el Protocolo Maker son la stablecoin o criptomoneda estable Dai, Maker Vaults colaterals, oráculos y votaciones. MakerDAO administra el protocolo Maker al decidir los parámetros fundamentales.

Además de la infraestructura del contrato inteligente, el protocolo Maker también incluye una variedad de actores externos para encargarse de las operaciones:

- *Los guardianes:* Un guardián es un actor independiente (por lo general automatizado) que se ve incentivado por las oportunidades de arbitraje para ofrecer liquidez en diversos aspectos de un sistema descentralizado. En el Protocolo Maker, los guardianes son participantes del mercado que ayudan a que las Dai conserven su precio objetivo ($ 1): ellos venden Dai cuando el precio del mercado está por encima del precio objetivo y las compran cuando el precio del mercado está por debajo del precio objetivo. Los guardianes participan en las subastas de excedentes, las subastas de deudas y las subastas de colaterales cuando se liquidan los Vaults.
- *Oráculos de precios:* El Protocolo Maker requiere información en tiempo real sobre el precio de mercado de los activos colaterales en las Maker Vaults para saber cuándo iniciar liquidaciones.

  El Protocolo obtiene sus precios colaterales internos de un oráculo de infraestructura descentralizada que es un conjunto amplio de nodos individuales denominados fuentes oráculo. Los votantes de MKR eligen un conjunto de fuentes de confianza para brindarle información de precios al sistema mediante transacciones Ethereum. También controlan cuántas fuentes forman el conjunto.

  Para proteger el sistema de un atacante que intenta obtener el control de la mayoría de los oráculos, el Protocolo Maker recibe los registros de precios mediante el Modelo de Seguridad de Oráculos (OSM, en inglés) y no directamente de los oráculos. El OSM, que es una línea de defensa entre los oráculos y el Protocolo, retrasa un precio durante una hora, lo que permite que los oráculos de emergencia o un voto de la Gobernanza de Maker congele a un oráculo si ha sido comprometido. Los tenedores de MKR son los responsables de tomar las decisiones sobre los oráculos de emergencia y la duración del retraso de los precios.
- *Oráculos de emergencia:* Los oráculos de emergencia son seleccionados por los votantes de MKR y actúan como la última línea de defensa contra un ataque al proceso de gobernanza o a otros oráculos. Los oráculos de emergencia pueden congelar oráculos individuales (por ejemplo, oráculos de ETH y BAT) para mitigar el riesgo de que un gran número de clientes intenten retirar sus activos del Protocolo Maker en un corto período, ya que tienen la autoridad para activar de forma unilateral un apagado de emergencia.
- *Equipos de DAO:* Los equipos de DAO constan de individuos y proveedores de servicios que pueden contratarse mediante la Gobernanza de Maker para brindarle servicios específicos a MakerDAO. Los miembros de los equipos de DAO son actores independientes del mercado y no empleados de la Fundación Maker.

  La flexibilidad de la Gobernanza de Maker permite que la comunidad de Maker adapte el marco del equipo de DAO para que se ajuste a los servicios requeridos por el ecosistema en función del rendimiento en el mundo real y los nuevos desafíos.

  Entre de las funciones de los miembros del equipo de DAO se encuentran el de facilitador de gobernanza, que brinda apoyo a la infraestructura de comunicación y los procesos de gobernanza, y los miembros del Equipo de Riesgo, que respaldan a la Gobernanza de Maker mediante la investigación de riesgos financieros y propuestas preliminares para incorporar nuevos colaterales y regular los ya existentes.

Se prevé que en un futuro cercano el DAO asuma el control total, lleve a cabo las votaciones de MKR y cumpla estas funciones variadas del equipo de DAO. (*Makerdao.Com*)

8.3. UNISWAP

Uniswap es un protocolo de intercambio de tokens descentralizado basado en Ethereum, el cual permite el intercambio directo de tokens sin necesidad de utilizar un intercambio centralizado. Al hacer uso de un intercambio centralizado, tendrá que depositar tokens en un intercambio, realizar un pedido en la libreta de pedidos y, a continuación, retirar los tokens intercambiados.

Para intercambiar tokens en Uniswap, se realiza desde una billetera, lo único que se necesita hacer es enviar tokens desde la billetera a la dirección de contrato inteligente de Uniswap y se recibirá el token solicitado en nuestra billetera. No hay ninguna libreta de pedidos y el tipo de cambio del token se determina algorítmicamente. Todo esto es posible a través de los grupos de liquidez y el mecanismo automatizado de creación de mercado.

Los grupos de liquidez son reservas de tokens que se encuentran en los contratos inteligentes de Uniswap, están disponibles para que los usuarios intercambien tokens. Por ejemplo, utilizando el par ETH-DAI con 100 ETH y 20.000 Dai en las reservas de liquidez, un usuario que quiera comprar ETH usando Dai puede enviar 202,02 Dai al contrato Uniswap para obtener 1 ETH a cambio. Una vez que el swap ha tenido lugar, el pool de liquidez se deja con 99 ETH y 20202,02 Dai.

Las reservas de grupos de liquidez son proporcionadas por proveedores de liquidez que son incentivados para obtener una tarifa proporcional de la tasa de transacción del 0,3% de Uniswap. Esta tarifa se cobra por cada intercambio de tokens en Uniswap.

El único requisito que se necesita para ser proveedor de liquidez es que una persona necesita proporcionar ETH y el token de trading cotizado a ser intercambiado al tipo de cambio Uniswap actual.

Los precios de los activos del grupo se determinan algorítmicamente mediante el algoritmo AMM o creador de mercado automatizado. AMM funciona manteniendo un producto constante basado en la cantidad de liquidez de ambos lados del pool. Para ello se usa esta ecuación:

$$x * y = k.$$

Figura 8.10. Ecuación para determinar el precio de compra y venta

Fuente:(Bit2me.Com)

Aquí la X e Y hacen referencia a la cantidad de tokens ETH y ERC-20 dentro del pool, y K es un valor constante. Esta ecuación utiliza el equilibrio entre los tokens ETH y ERC-20, y la oferta y la demanda, para determinar el precio de un token en particular.

Continuando con el grupo de liquidez ETH-DAI. 100 ETH Y 20000 DAI. Para calcular el producto constante, Uniswap multiplicará ambas cantidades juntas.

Liquidez de ETH (100) *liquidez DAI (20000) = producto constante (2000000) (k)

Utilizando AMM, en un momento dado, k siempre debe permanecer en 2000000. Si alguien compra ETH usando DAI, ETH se eliminará del grupo de liquidez, mientras que DAI se agregará al grupo de liquidez.

El precio de esta ETH se determinará asintóticamente. Cuanto mayor sea el pedido, mayor será la prima que se cobra.

A diferencia de los intercambios centralizados, Uniswap como es un intercambio descentralizado no tiene un equipo para evaluar y decidir qué tokens enumerar. En su lugar, cualquier token ERC-20 puede ser listado en Uniswap por cualquier persona y ser negociado siempre y cuando exista liquidez para el par dado. Todo lo que un usuario necesita hacer es interactuar con la plataforma para registrar el nuevo token, dando lugar al inicio de un nuevo mercado para este token.

El token UNI tiene varios casos de usos, el primer caso de uso del token UNI es que se utilice como token de gobernanza. Esto permite que todos los titulares de UNI voten sobre cuestiones clave que pueden tener un impacto serio en la dirección que toma Uniswap, lo que en última instancia puede tener un gran impacto en la acción del precio (PA). La gestión de la tesorería estará a cargo de la comunidad, lo que es un buen augurio para los titulares de UNI.

Por otro lado, El token UNI también proporcionará liquidez en Uniswap, ya que los proveedores de liquidez (LP) pueden proporcionar su UNI junto con una cantidad equivalente de ETH para tomar una parte de todas las tarifas pagadas cuando un usuario compra o vende tokens. (Lau et al., 2020)

8.4. BALANCER

Balancer es un software que se ejecuta en Ethereum, funciona como un creador de mercado automatizado con ciertas propiedades claves que hacen que funcione como una cartera ponderada y un sensor de precios auto equilibrados. El objetivo es incentivar una red distribuida de computadoras para operar un intercambio donde los usuarios pueden comprar y vender cualquier criptomoneda.

Balancer le da la vuelta al concepto de fondo indexado, en lugar de pagar tarifas a los administradores de cartera para reequilibrar su cartera, cobra tarifas de los comerciantes, que reequilibran su cartera siguiendo las oportunidades de arbitraje.

En balancer podemos encontrar dos usuarios:

- *Proveedores de liquidez*: Son aquellos que actúan como propietarios de los pools y aportan sus activos en ellos para ofrecer swaps eficientes y baratos a los traders. Generan un rendimiento de capital a través de tarifas, además de tener un servicio remunerado de gestión de activos ya que puedes participar o crear en el todo tipo de pools, con tokens y distribuciones completamente distintas.
- *Traders*: Estos usan los pools como servicio de Exchange para hacer swaps entre tokens. Estos además pueden usar el protocolo para realizar arbitraje.

Balancer ofrece pools públicos, pools privados y pools inteligentes. Los pools públicos permiten que cualquier usuario proporcione liquidez agregando o retirando activos. Cabe destacar que los parámetros de las piscinas públicas se establecen y no se pueden cambiar antes de su lanzamiento. Este tipo de pools suele ser útil para usuarios más pequeños que buscan obtener tarifas de los grupos más populares y líquidos. Por otro lado, nos encontramos con los pools privados, en el que solo el creador del grupo puede agregar o retirar activos. El usuario también puede ajustar

todos los demás parámetros del grupo, como tarifas, ponderaciones y los tipos de activos que acepta. Los pools privados suelen ser útiles para los administradores de activos con una gran cartera que buscan ganar comisiones por sus activos específicos. Por último, los pools inteligentes, son controlados por contratos inteligentes y pueden implementar cualquier estrategia o lógica comercial arbitraria. (*Kraken.Com*)

Balancer permite usar pools con proporciones como 95/5. 95% del valor en tu propio token y el 5% en otro token como ETH o Dai. Esto te permite dar liquidez a tu token sin necesidad de contar con muchos recursos.

A nivel de protocolo, la base de las funciones de intercambio de Balancer es una superficie definida por la restricción de una función de valor. V- una función de los pesos y equilibrios de la piscina - a una constante. Esta superficie implica un precio spot en cada punto de manera que, independientemente de los intercambios que se realicen, la participación de valor de cada token en el pool permanece constante.

La función de valor V Se define como:

$$V = \prod_t B_t^{W_t}$$

Figura 8.11. Función valor de V

Fuente: (*Balancer.Finance*)

Donde:

- T se extiende sobre las fichas en la piscina.
- Bt es el saldo de la ficha en la piscina.
- Wt es el peso normalizado del token, de manera que la suma de todos los pesos normalizados es 1.

De esta forma haciendo V constante podemos definir una superficie de valor invariante.

Por último, un concepto importante a tener en cuenta es el deslizamiento de precios, el cual consiste en cuanto puede variar el precio del swap en función del estrés que está asumiendo el pool. Por ejemplo, si yo quiero swapear 1ETH por DAI y el pool es muy líquido, si 1ETH = 100DAI, seguramente el swap me aportará 100 DAI. Ahora bien, si queremos swapear 1000ETH seguramente no vamos a recibir 100.000DAI, ya que habremos puesto demasiado estrés al pool y este estará cobrando un precio de cambio más alto.

Por tanto, los pools más eficientes en cuanto a deslizamiento de precios son los pools 50/50, lo cual se puede demostrar a través del siguiente gráfico.

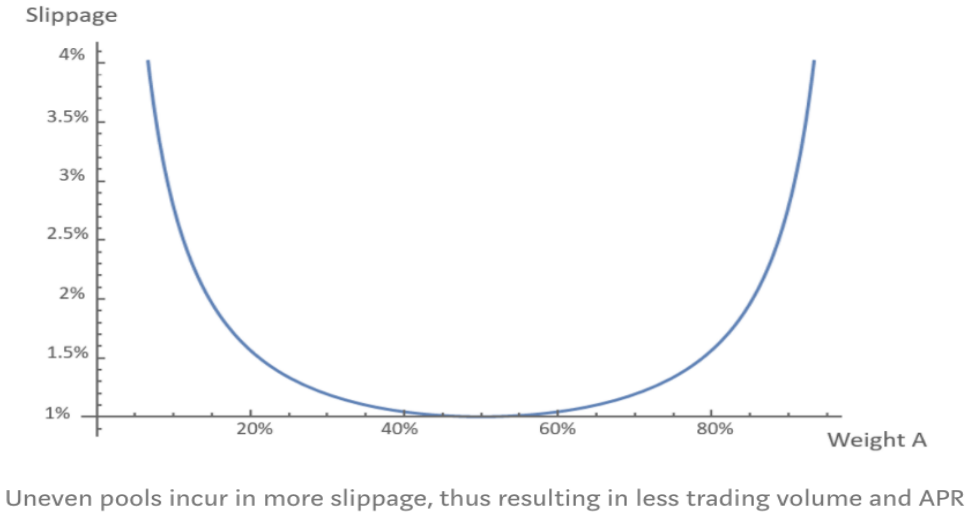

Figura 8.12. Pools más eficientes en cuanto al deslizamiento de precios

Fuente: (*Criptoblog.Tutellus.Com*)

Pools desiguales provocan un deslizamiento de precios mayor, dando como resultado menos volumen tradeado y por tanto un retorno anual inferior. Esto podría ser una desventaja para Balancer en comparación a Uniswap mientras los costes de gas sigan siendo tan altos. (*Criptoblog.Tutellus.Com*)

8.5. CURVE

Curve es un protocolo de intercambio descentralizado basado en Ethereum, dedicado a ofrecer intercambios de monedas estables o stablecoins. Este protocolo realiza operaciones como las de Uniswap, con la diferencia que Curve se centra en activos con paridad 1 a 1.

El funcionamiento de Curve puede entenderse como un Exchange descentralizado. Pero detrás de este Exchange hay algunos conceptos como los pools de liquidez, los cuales son los que permiten tener la liquidez necesaria para sus intercambios de stablecoins.

Los usuarios de los pools de liquidez inyectan liquidez con el fin de obtener ganancias provenientes de los préstamos o intercambios que se realizan usando estos activos. Así, cada préstamo o intercambio realizado lleva un interés, que sumados en total termina por alimentar las ganancias de los proveedores de liquidez.

De esta forma los proveedores de liquidez pueden inyectar su DAI O USDT a las Curve pools, que luego este protocolo usará para ofrecer intercambios con un ligero interés, el cual alimentará las ganancias de los proveedores de liquidez. El hecho de que el protocolo use stablecoins, hace que incluso cada decimal cuente y, al final, la ganancia obtenida sea importante en relación con el tiempo que se bloquee un determinado capital dentro del pool.

La ratio de intercambio manejado dentro del pool es administrado de forma autónoma por contratos inteligentes. De esta forma, por ejemplo, si un pool ofrece intercambios DAI/USDT y existe en ella paridad entre sus tokens (hay 1000 DAI y 1000 USDT), la ratio del intercambio será de 1:1. Sin embargo, si esa ratio cambia por ejemplo 800 DAI y 1200 USDT, la ratio del intercambio iría subiendo para el DAI y bajando para el USDC, todo con la finalidad de que el pool vuelva a equilibrarse y siempre cuente con liquidez para sus operaciones.

Además de esto, Curve se integra también con otras plataformas, proporcionando otro medio de intercambio secundario con el fin de obtener mayores ganancias. Esta es la razón por la que podemos ver pools de liquidez en proyectos como Yearn Finance, Uniswap o Compound, cada uno de ellos pensados en sacar provecho de la liquidez contenida en Curve, usando dichos activos en otros protocolos.

El token de gobernanza de curve es CRV, el cual ha sido diseñado para para incentivar a los proveedores de liquidez de la plataforma, así como para lograr la mayor cantidad de usuarios involucrados en la gobernanza del protocolo.

El token CRV tiene una oferta total de 3,03 billones que se distribuirán de la siguiente forma:

- 62% a proveedores de liquidez comunitarios.
- 30% a accionistas (equipo e inversores) con 2-4 años de consolidación.
- 3% a empleados con 2 años de consolidación.
- 5% a la reserva comunitaria.

Entre los 1300 millones de CRV (43% del total) se distribuirá en la emisión inicial de la siguiente forma:

- 5% a proveedores de liquidez anteriores a CRV con derecho a 1 año.
- 30% a accionistas (equipo e inversores) con 2-4 años de consolidación.
- 3% a empleados con 2 años de consolidación.
- 5% a la reserva comunitaria.

Al comienzo del lanzamiento, la circulación de CRV era 0 y la tasa de liberación inicial era de aproximadamente de 2 millones de CRV por día. (*Bit2me.Com*)

8.6. COMPOUND

Compound es un protocolo de mercado monetario en la cadena de bloques de Ethereum. Estos mercados monetarios, son grupos de activos con tasas de interés derivadas algorítmicamente, basadas en la oferta y la demanda del activo. Cuando la liquidez es abundante, las tasas de interés son bajas, a medida que la liquidez se vuelve escasa, las tasas de interés aumentan.

Los proveedores y prestatarios de un activo interactúan directamente con el protocolo, ganando o pagando una tasa de interés flotante, sin tener que negociar términos como vencimiento, tasa de interés o garantía con un par o contraparte.

Cada mercado monetario es único de un activo Ethereum. Estos contienen un libro mayor transparente e inspeccionable públicamente, con un registro de todas las transacciones y tasas de interés históricas.

El protocolo Compound opera como un pool de liquidez. Los proveedores suministran activos a la piscina y ganan intereses, mientras que los prestatarios toman un préstamo de la piscina y pagan intereses de su deuda.

Los activos suministrados a un mercado están representados por un saldo en un token ERC-20, conocido como cToken, que da derecho al propietario a una cantidad cada vez mayor del activo subyacente. Esto es posible, debido a que el mercado monetario, a medida que acumula intereses, cToken se convierte en convertible en una cantidad cada vez mayor del activo subyacente.

Compound permite a los prestatarios pedir prestado sin fricción en el protocolo, utilizando cToken como garantía de estos préstamos. El factor colateral va de 0 a1 y representa la porción del valor de activo subyacente que se puede pedir prestado.

Si el valor del activo que hemos dejado en el protocolo como garantía sube, la ratio de garantía también sube, lo que nos permitirá pedir un prestamos más grande. En caso contrario, si el valor del activo que hemos dejado como garantía baja, la ratio de garantía también baja, situándose por debajo de la relación de garantía requerida, la garantía se venderá parcialmente junto con una tarifa de liquidación del 5%. Este proceso de liquidación se lleva a cabo para alcanzar la relación de garantía mínima, de esta forma el protocolo se asegura siempre que haya exceso de liquidez para el retiro y préstamo de fondos.

Por último, la gobernanza de Compound es administrada por una comunidad descentralizada de poseedores de tokens COMP y sus delegados, quienes proponen y votan las actualizaciones del protocolo. (Leshner & Hayes, 2018)

8.7. AAVE

Aave es un protocolo de mercado de liquidez descentralizado sin custodia, donde los usuarios pueden participar como depositantes o prestatarios. Los depositantes son los encargados de proporcionar liquidez al mercado para obtener un ingreso pasivo, mientras que los prestatarios pueden pedir prestado en forma sobrecolaterizada o subcoleratizada.

El protocolo Aave crea aTokens al depositar un activo y son quemados cuando se canjean. Estos aTokens están vinculados 1:1 al valor del activo subyacente que se deposita en el protocolo. Estos aTokens se pueden almacenar, transferir e intercambiar libremente.

Las liquidaciones en el protocolo sirven para determinar el estado de salud de un préstamo, dando lugar a dichas liquidaciones cuando el valor del activo que hemos dejado como garantía baja de los niveles de la garantía requerida. En función del riesgo del activo la penalización por ser liquidado puede rondar entre el 5% y el 15%.

Algo interesante del protocolo de Aave es la integración en la propia plataforma de un servicio de liquidación, para dar más equilibrio al protocolo. Gracias a esta integración cualquiera puede liquidar préstamos y recibir “dinero gratis” por ello. Claro está que estas oportunidades no suelen estar disponibles porque los bots se encargan de liquidar cualquier préstamo rentable en el momento que aparece.

El tipo de interés funciona según la oferta y la demanda, por tanto, el precio del dinero que hemos pedido puede variar en el tiempo. Cuanta más liquidez haya en el protocolo menos bruscos serán estos cambios, pero en casos excepcionales los tipos de interés pueden llegar a dispararse. Este riesgo puede ser mitigado eligiendo un tipo de interés fijo, el cual es más alto que el que proporciona el protocolo en ese momento.

La innovación que presenta Aave con respecto a Compound son los préstamos flash. Estos son la primera opción de préstamo sin garantía en DeFi. Los prestamos flash son un préstamo que puedes pedir al protocolo de Aave sin necesidad de poner nada como garantía, siempre que el préstamo se pague de vuelta por completo más un 0,09% de comisión en esa misma transacción. Si el préstamo no se devuelve en esa misma transacción es cancelada, por tanto, no se llega a emitir.

Este tipo de préstamos es principalmente usado por desarrolladores que integran esta liquidez en sus aplicaciones para ofrecer servicios con ellos, que suelen tener el

objetivo de generar dinero a través del arbitraje o de ahorrar dinero autoliquidando préstamos obtenidos.

Por último, cabe destacar que Aave no se limita a ser un protocolo de préstamo, sino más bien un protocolo de mercados financieros, donde la opción de pedir y depositar es solo uno de los mercados disponibles.

Un segundo mercado de Aave consiste en usar como garantía los tokens liquidados de Uniswap. Con esta integración de Aave ahora se puede usar como colateral los tokens de liquidez y tomar un préstamo. Este mercado es más arriesgado que el de préstamo por el tipo de token usado para colateralizar, además del hecho que Uniswap tiene un riesgo intrínseco debido al rebalanceo de entre los dos tokens depositados en el pool. (*Criptoblog.Tutellus.Com*)

8.8. YEARN FINANCE

Yearn.Finance es un protocolo de préstamos descentralizados de código abierto, basado en la cadena de bloques de Ethereum, que permite a los usuarios maximizar sus propias ganancias, sobre los activos criptográficos, a través de servicios de préstamos y trading.

Funciona como una plataforma de agregación de la rentabilidad para maximizar la inversión del usuario moviendo automáticamente los fondos del usuario entre los protocolos de préstamo DeFi (como Compound, Curve o Aave).

Por tanto, podemos decir que Yearn.Finance es un administrador de liquidez, que busca automáticamente el mejor porcentaje de rendimiento anual, teniendo siempre en cuenta el nivel de riesgo con el que el cliente está dispuesto a trabajar.

Yearn.Finance está diseñado para mover de forma automática y autónoma los fondos de los usuarios a los proveedores más rentables identificando el protocolo que ofrece el mejor porcentaje de rendimiento anual (APY).

Los clientes del protocolo proporcionan liquidez que se desvía automáticamente a diferentes sectores de las finanzas descentralizadas para encontrar los mejores rendimientos.

Dependiendo del riesgo, la plataforma decidirá proporcionar liquidez donde sea más rentable, optimizar la búsqueda de la mejor rentabilidad posible y moviendo los fondos cuando un proyecto DeFi, con el mismo riesgo, tendrá rendimientos más altos.

Yearn.Finance permite a los usuarios depositar stablecoin ERC-20 como DAI, USDC, USDT, en el protocolo. A cambio, los usuarios reciben una cantidad equivalente de yToken (por ejemplo, yDAI, yUSDC, yUSDT) que es equivalente a cualquier otro token ERC-20.

Por lo tanto, la plataforma Yearn Finance convierte automáticamente los tokens en un protocolo con el máximo rendimiento para maximizar el beneficio del usuario.

Uno de los aspectos más interesantes es que la red sólo cobra una pequeña tarifa por el depósito en el pool de la plataforma y que se distribuye entre los titulares de token YFI como dividendos.

YFI es la criptomoneda nativa de Yearn.finance que se diferencia de la mayoría de las criptomonedas por ser un token de gobernanza sin ningún valor intrínseco y que cuenta con un protocolo independiente.

Además, a diferencia de otras criptomonedas, no puede ser minada.

YFI se distribuye a aquellos usuarios que brindan liquidez a cualquiera de las plataformas que utilizan los yTokens y su finalidad es otorgar la entera gobernanza del

sistema yEarn a la comunidad, ya que permite a los titulares votar las decisiones que afectan a Yearn.

Esto significa que los usuarios de la plataforma tienen derecho a votar sobre la gestión del protocolo que más favorece sus necesidades.

- Para participar en el protocolo, los usuarios primero tienen que invertir sus tokens YFI en un contrato de gobierno.
- Una vez invertidos sus YFI, reciben derechos de voto y un porcentaje de las ganancias del protocolo para cada uno de los productos de Yearn.
- Para desbloquear y recibir las recompensas, los usuarios tendrán que votar y, después de tres días, recibirán las recompensas ganadas.

En relación al suministro de YFI, solo hay 30,000 token YFI y, hasta la fecha, se han acuñado y distribuido ya 29,969 YFI (sólo faltan 31 tokens por emitir). (*Blog.Bitnovo.Com*)

CAPÍTULO 9: EL CASO DEL MERCADO BLOCKCHAIN DE FUTUROS DEL ACEITE DE OLIVA

La problemática económica y financiera del sector del aceite de oliva, el modelo de volumen y precio dominante en la actualidad, ha convertido al mercado español del aceite de oliva en un producto indiferenciado, de escaso valor. En este escenario, las virtudes del producto se difuminan y el aceite de oliva pasa a ser considerado como una grasa alimenticia indiferenciada. Y es así como el mercado español ha acabado por estar dominado en un 65% por las marcas blancas, lo cual responde a que este sector esté basado en volumen y precios alejados del concepto de calidad, como es el que debería primar. Sin embargo, cuando el 95% de los consumidores mundiales lo son de grasas cinco veces más baratas que el aceite de oliva, competir en precios es una batalla perdida.

Pero lo más preocupante es que este modelo de comercialización que domina el mercado español se está empezando a replicar peligrosamente en otros mercados, que a priori, tienen un gran potencial para el consumo de aceite de oliva y que, hasta ahora, eran mercados de margen, como Estados Unidos, Reino Unido, Alemania u Holanda. Esta situación ha llevado al sector a una situación económica límite donde más del 90% de los ingresos de explotación que genera equivalen a la compra de aceitunas y otros costes de aprovisionamiento, con lo que un gran número de pequeñas empresas olivareras y almazaras productoras se plantean el cierre si no cambian las actuales circunstancias.

Otro de los problemas a tener en cuenta en este sector es la logística del aceite de oliva, la cual sufre una serie de ineficiencias causadas por procesos obsoletos que la cadena de bloques podría solucionar. Alguno de los numerosos problemas existentes en la logística del sector olivarero son la falta de transparencia causada por los distintos sistemas, los altos costes de procesos que, además, son lentos y manuales y las dificultades relacionadas con la cantidad de tiempo requerido para crear y cerrar un contrato.

Por otro lado, en España, el mercado nativo de futuros del aceite de oliva ha desaparecido por completo debido a regulaciones y requisitos muy estrictos impuestos por los reguladores locales. Combinado con un mercado muy volátil para los productores del aceite de oliva, debido a la Covid-19, esta situación ha causado un gran daño financiero a los productores de aceite de oliva que no pudieron cubrir sus riesgos de producción utilizando derivados.

Todo lo comentado anteriormente está ocasionando que los productores de aceite de Andalucía (líder en producción oleícola a nivel mundial, con el 80% de la cosecha nacional) no dispongan de un mecanismo transparente y no consigan repercutir los costes en el precio y puedan incluso perder dinero.

De esta forma surge el mercado blockchain de futuros sobre el aceite de oliva, la idea inicial se centró en lanzar su propia criptomoneda, Olivacoin, pero el equipo le ha dado un giro al proyecto hacia la idea de crear contratos de futuros del aceite de oliva totalmente descentralizados, creando un mecanismo de mercado para la fijación de precios más transparente gracias a blockchain.

En lugar de lanzar su propia infraestructura desde cero, han lanzado su producto en el protocolo Opio, ya que de esta forma se reducen costes y los esfuerzos necesarios para su salida al mercado.

El mercado blockchain de futuros sobre el aceite de oliva es uno de los cuatro proyectos externos que tienen como objetivo llevar sus ideas derivadas a Opium. Al aprovechar el sistema del Protocolo de Opium, este mercado blockchain de futuros ahorrará millones en el proceso de emisión e intermediación, que se simplificará en cuestión de minutos, además de ganar notablemente en la transparencia de la formación de precios.

Opium Exchange, es una plataforma de derivados descentralizada construida sobre Ethereum. Opium es un sistema complejo que tiene como objetivo proporcionar una experiencia fácil de uso para las masas. Los derivados descentralizados tienen muchas ventajas con respecto a los tradicionales, especialmente en materia de acceso, tarifas y seguridad.

Gracias a la infraestructura de Opium Exchange, cualquier persona puede emitir y negociar instrumentos de derivados descentralizados, como futuros u opciones, sin ningún riesgo de contraparte en un entorno sin permisos, que puede ayudar a los usuarios minoristas a eludir las restricciones locales y tomar el control total de su libertad financiera. Además, los emisores de derivados también se beneficiarán de precios más bajos y tiempos de emisión más rápidos.

El protocolo Opium traerá muchas oportunidades al mundo de DeFi, permitiendo que cualquiera pueda emitir cualquier tipo de derivado.

Una vez que hemos fundamentado el propósito de este producto, vamos a explicar cómo obtenerlo. Los derivados del aceite de oliva descentralizados no son una idea, es un producto fácilmente disponible que ahora se puede probar en Opium Exchange. A continuación, se muestran los pasos a seguir para intercambiar estos productos:

En primer lugar, nos vamos a ir a test.opium.exchange y procederemos a conectar nuestra wallet.

Una vez que hemos elegido y conectado la wallet, para comenzar a operar en papel, debemos adquirir algunas monedas DAI de prueba. Para ello, debemos comunicarnos con Opium y proporcionar la dirección de nuestra billetera en Rinkeby Test Network. Una vez hecho esto, los miembros del equipo de soporte envían las monedas DAI de prueba directamente, para que estas sean usadas en operaciones de prueba. Completado este paso, pasaremos a habilitar los tokens DAI de prueba para facilitar los intercambios que especificaremos posteriormente. Tras esto debemos permitir que el intercambio de Opio gaste el DAI.

Llegados a este punto nos trasladaremos a la página intercambio y estaremos listos para operar.

Una vez situados en la página de intercambio tenemos que encontrar y elegir el ticker de futuros de Oliva. Cada ticker tiene una descripción de los términos del contrato en la

página de Exchange y una descripción detallada en la página del Explorador de Derivados.

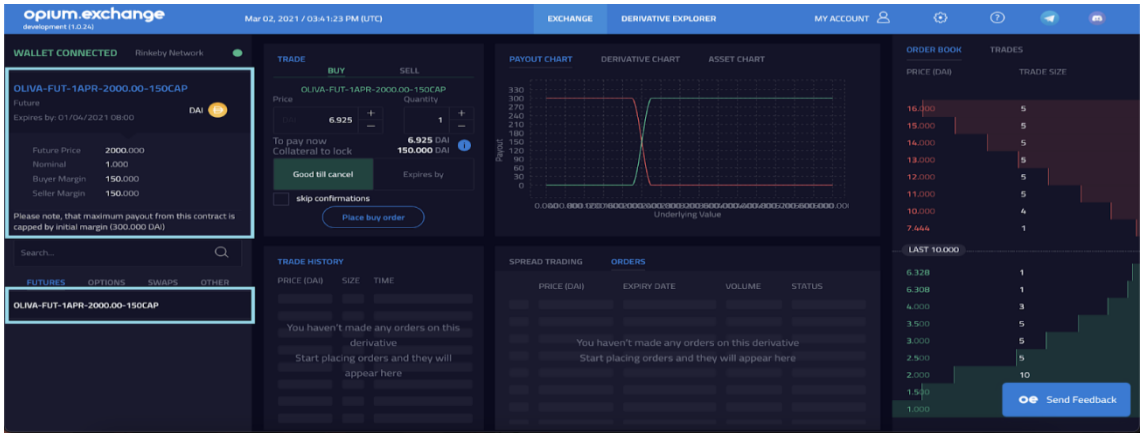

Figura 9.13. Ticker de los futuros del aceite de oliva

Fuente: (Medium.Com)

En la sección intercambiar podemos elegir el precio, la cantidad a intercambiar y realizar la orden de compra.

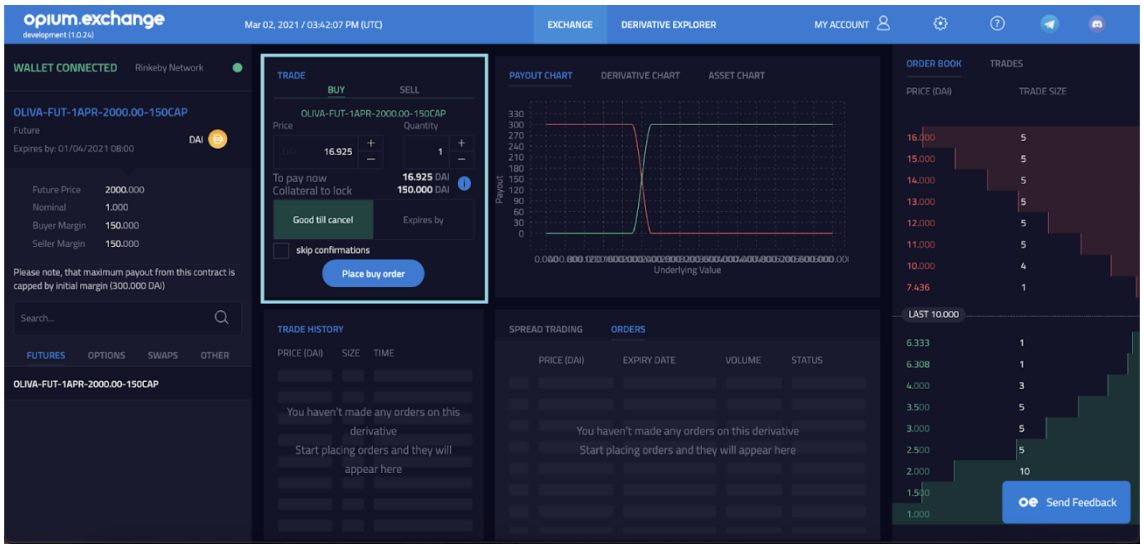

Figura 9.14. Panel de precios, cantidad a intercambiar y orden de compra

Fuente: (Medium.Com)

Posteriormente, aparecerá una ventana emergente con información detallada sobre el pedido realizado.

Las ordenes que pertenecen abiertas son visibles en la sección "órdenes". Cada pedido se entrega instantáneamente al libro de pedidos, pero cuando se liquida, necesita la cadena de bloques para confirmarlo. Es por eso que las ejecuciones de los asentamientos tardan unos segundos en la confirmación final y sin confianza.

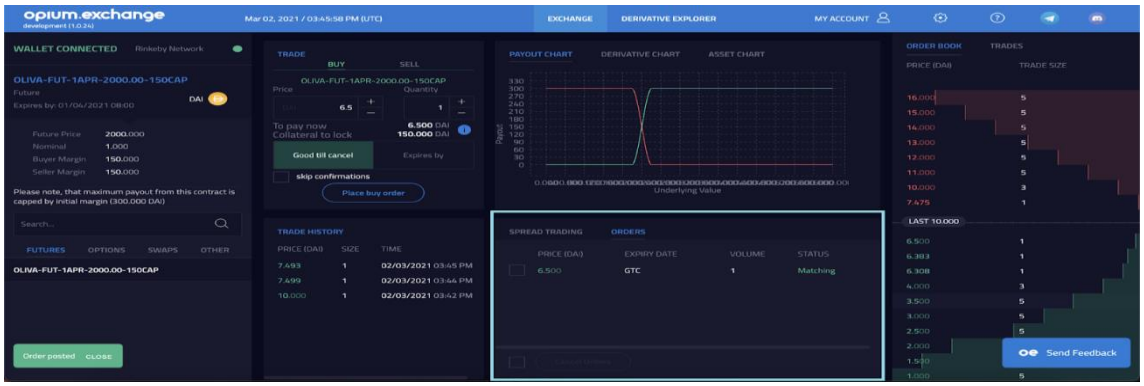

Figura 9.15. Número de ordenes abiertas

Fuente: (Medium.Com)

Después de que el pedido sea igualado, el intercambio se confirmará en la cadena de bloques Ethereum. La operación aparecerá en la sección historial de operaciones.

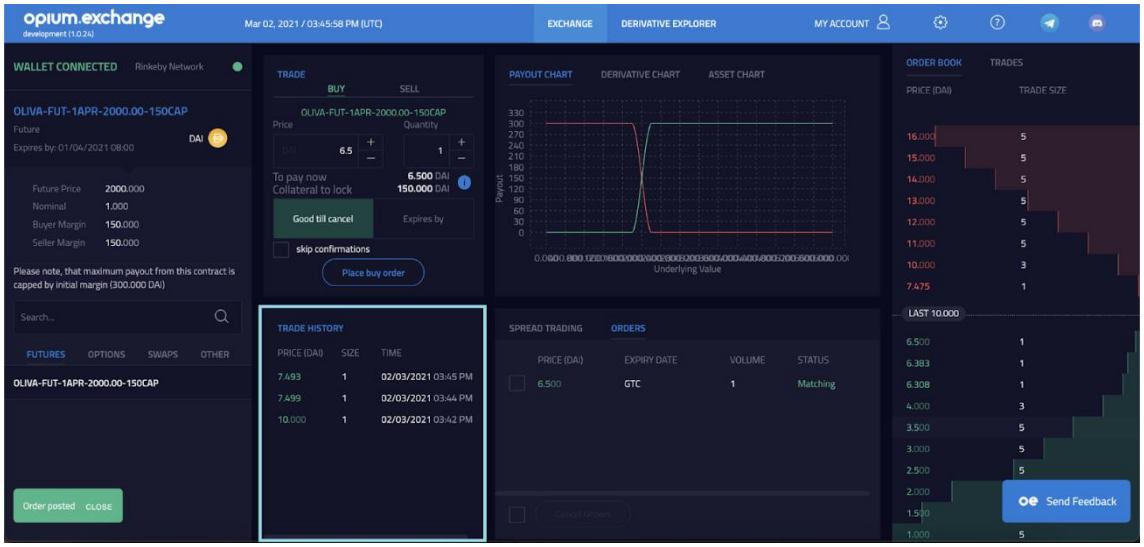

Figura 9.16. Operaciones confirmadas en la sección historial de operaciones

Fuente: (Medium.Com)

Cuando el pedido aún no se ha correspondido, aún puede ser cancelado. Una vez que la operación se liquide en la cadena de bloques, no podrá ser cancelada.

Una vez que hemos comprado un derivado, se muestra en "Mi cuenta" en la pestaña "Derivados". Podemos ver la cantidad de contratos que tenemos, el ticker, el tipo de posición (larga o corta) y realizar algunas acciones: envolver varias posiciones en un token de cartera (para operar con él como una posición), enviar tokens a otra dirección o puesto en ejecución vencido (para recibir su ganancia o pérdida).

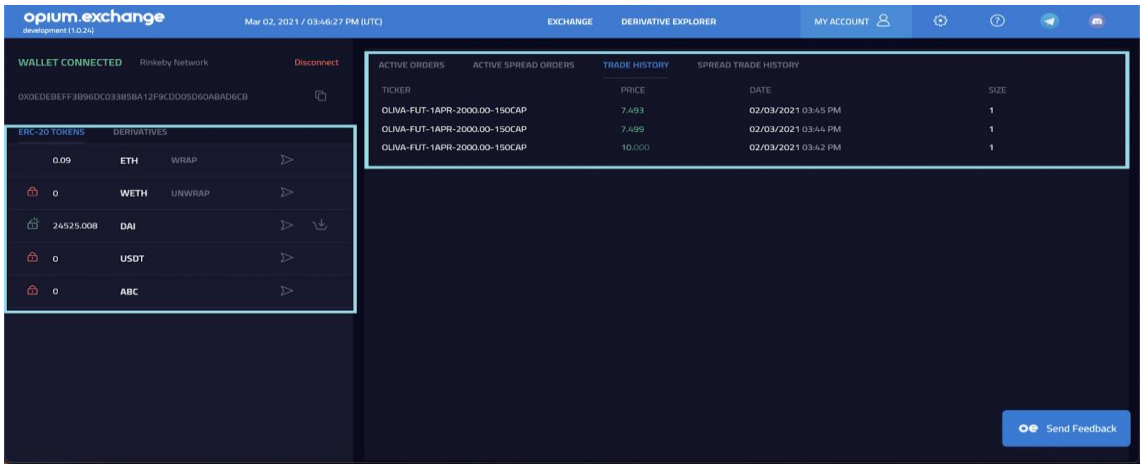

Figura 9.17. Cantidad de contratos en posesión, ticker, tipo de posición y otras acciones

Fuente: (Medium.Com)

Para empezar, tenemos que decir que un contrato de futuros es un acuerdo de compromiso para hacer entrega o recibir una determinada mercancía que tiene estandarizados todos los aspectos excepto el precio, que se negocia en el mercado. La gran mayoría de contratos abiertos (95-97% del total) no llegan a vencimiento –se compensan antes de esa fecha– y no dan lugar a ninguna entrega real del «bien subyacente», en nuestro caso, el aceite de oliva virgen extra.

En relación al funcionamiento, podemos decir que para abrir una posición –compradora o vendedora– en cualquier mercado de futuros, se debe depositar una garantía inicial –también llamada garantía por posición abierta, depósito de garantía o margen inicial– en la Cámara de Compensación del mercado. Una vez cerrada la operación, es decir, una vez cumplido el compromiso en el vencimiento y cerrada la posición, la Cámara devolverá esa garantía inicial. Para cerrar una posición en futuros antes del vencimiento, se realiza la operación contraria:

• Si la posición abierta es larga, para cerrarla se venden futuros.

• Si la posición abierta es corta, para cerrarla se compran futuros.

De esta manera desaparecerá el riesgo de incumplimiento y, por tanto, la Cámara de Compensación libera el depósito de garantía por posición abierta.

A continuación, veremos un ejemplo de cobertura de precios sobre el aceite de oliva virgen extra:

Ejemplo Cobertura. 1 DAI = 1$ EE.UU.		
Objetivo	Quiere asegurarse un precio AOVE de compra para septiembre de:	3.000 $
Actuaciones en MFAO	Compró en Agosto Contrato v to. Septiembre	3.000 DAI
	Cierra posición: Vende contratos v to. Septiembre a:	3.020 DAI
	Ganancia en Mercado Futuros :	+ 20 DAI
Actuaciones en contado	Ahora compra AOVE al contado 20 $ más caro a:	3.020 $
Precio al que realmente realiza la operación coincide con su Objetivo		3.000 $

Figura 9.18. Ejemplo de cobertura de precios sobre el aceite de oliva virgen extra

Fuente: (Santiago Moreno, 2021)

En definitiva, este mercado blockchain de futuros sobre el aceite de oliva lo que pretende es aprovechar la oportunidad de liderazgo que dispone el mercado español en la producción mundial del aceite de oliva, cuyos objetivos se podrían concretar en los siguientes: poner en valor el aceite de oliva virgen extra desde en el contexto internacional y a un público joven nativo de Internet, ayudar a los participantes del mercado a protegerse contra los riesgos causados por la volatilidad de los precios de los productos del aceite de oliva mediante la posibilidad de contratos de cobertura de precios, proporcionar transparencia de precios con garantía y trazabilidad blockchain, contribuir al cumplimiento de la ley de la cadena alimentaria al facilitar a los productores no vender a pérdidas, aportar gran cantidad de liquidez por parte de criptoinversores globales de todo el mundo y conseguir una difusión y promoción mundial no conocida hasta la fecha del aceite de oliva.

CAPÍTULO 10: CONCLUSIONES

A través de la elaboración de este Trabajo Fin de Grado hemos podido analizar la mecánica de la tecnología blockchain y enlazarla con la aplicación que tiene esta en el ecosistema DeFi.

El nuevo paradigma que suponen las finanzas descentralizadas, constituye un ingrediente indispensable de la nueva infraestructura global de los servicios financieros. La tecnología que sustenta a DeFi, proporciona importantes ventajas competitivas que están permitiendo una considerable expansión de estos protocolos, cuyo mayor ejemplo ha sido Bitcoin. De forma similar, Ethereum se ha consolidado como la plataforma para implementar servicios financieros descentralizados.

Aunque estas criptomonedas y los servicios que ofrecen sus aplicaciones puedan estar sometidos a una cierta volatilidad, su tecnología descentralizada nos proporciona una alternativa a las entidades financieras.

Desde su aparición, blockchain está captando la atención de muchas actividades empresariales, esto se debe a la multitud de posibilidades que abre esta tecnología, que van desde la reducción de costes para las empresas, mejoras en la prestación de servicios, transparencia, rapidez y confianza en las transacciones comerciales entre empresas y particulares.

Con la llegada de blockchain al ámbito empresarial, se están tratando de resolver problemas como los que presenta el mercado del aceite de oliva, surgiendo así, el primer mercado descentralizado de futuros del aceite de oliva, construido sobre la red Ethereum. En este mercado, el volumen de operaciones representa aún un porcentaje pequeño con respecto a los volúmenes negociados en el mercado de contado, por lo que resulta necesario un mayor compromiso y de negociación por parte de los operadores que actúan en el mercado físico, con el objetivo de que la liquidez y la negociación en este mercado aumente, lo que dará lugar a una consolidación del papel que pretende representar el mercado de futuros descentralizado como referencia de precios.

El crecimiento del volumen de operaciones de este mercado va a depender de que las empresas del sector del aceite oliva, vean la oportunidad de cubrirse en precios y así no incurrir en pérdidas en su producción, lo cual no es legal en España según la ley de cadena alimentaria.

Este proceso será lento, ya que los productores de aceite de oliva tienen un gran desconocimiento acerca de las criptomonedas y los protocolos DeFi, hecho que viene provocado por la temprana edad de las criptomonedas y de dichos protocolos, a lo que hay que sumar que estos no disponen aun del peso que tienen los mercados tradicionales. Sin embargo, las criptomonedas y los principales protocolos DeFi pueden jugar un papel importante en el futuro, por lo que es necesario que los productores de aceite de oliva comiencen a indagar en estos mercados.

Por otro lado, la crisis financiera y todos sus efectos han provocado que la confianza de la población en el sistema bancario sea muy baja, ya que por ejemplo en países como Argentina, muchas personas han visto sus depósitos congelados por los bancos, además, su moneda sufre una elevada inflación, por lo que, debido a esta situación, ven en la moneda digital un medio para preservar su patrimonio, lejos de un nuevo colapso del sistema bancario.

En definitiva, DeFi tiene el potencial de cambiar el panorama financiero actual de manera positiva. ¿Quién va a querer montar una empresa, si puedes crear una DAO? Los protocolos DeFi, gracias a los algoritmos matemáticos y los Smart Contract funcionan mejor que la gestión de los humanos. Un claro ejemplo sería Compound.

La grandeza de la descentralización gracias a blockchain es que uno es libre y total propietario de lo que es suyo. Sin corralitos y sin confiscaciones. DeFi todavía es un mercado pequeño y tiene un largo camino por recorrer. Con nuevos proyectos y protocolos que ingresan al mercado, el mundo puede esperar un verdadero sistema financiero descentralizado en los próximos años. Esto es el fin de una era y el comienzo de otra nueva.

BIBLIOGRAFÍA

Demirors, M., & Sheffield, C. (2020). Crypto , What Is It Good For? An Overview of Cryptocurrency Use Cases. *World Economic Forum Global Future Council on Cryptocurrencies*, *December*.

González Otero, J. M., Moreno de la Cova, F., & Gutiérrez García, E. (2013). *Bitcoin : la moneda del futuro : qué es, cómo funciona y por qué cambiará el mundo* . Unión Editorial.

https://academy.binance.com/es/articles/what-is-tether-usdt

https://academy.bit2me.com/cuantos-tipos-de-blockchain-hay/

https://academy.bit2me.com/que-es-curve-crv/

https://academy.bit2me.com/que-es-usdt-theter-criptomoneda/#:~:text=El 20 de noviembre de,pasaría a denominarse “Tether“.

https://academy.bit2me.com/que-es-uniswap/

https://balancer.finance/whitepaper/#swap-and-exit-fees

https://blog.bitnovo.com/que-es-yearn-finance/#:~:text=Lanzado en febrero de 2020,servicios de préstamo y trading.

https://coinmarketcap.com/es/currencies/ethereum/

https://criptoblog.tutellus.com/entendiendo-balancer-por-completo/

https://criptoblog.tutellus.com/entendiendo-aave-protocol/

https://defipulse.com/

https://es.cointelegraph.com/explained/defi-what-it-is-and-its-impact-on-the-crypto-world

https://es.cointelegraph.com/explained/how-the-bitcoin-exchange-rate-is-calculated

https://hackernoon.com/how-decentralized-is-defi-a-framework-for-classifying-lending-protocols-90981f2c007f

https://makerdao.com/es/whitepaper/

Https://makerdao.com/whitepaper/Dai-Whitepaper-Dec17-es.pdf. (2017). *El sistema Dai Stablecoin*.

https://medium.com/opium-network/oliva-futures-on-oex-f2ef6ff67c7d

https://medium.com/stably-blog/decentralized-finance-vs-traditional-finance-what-you-need-to-know-3b57aed7a0c2

https://nexusmutual.io/token-model.html

https://tokentuesdays.substack.com/p/nexus-mutual

https://www.bbva.com/es/que-son-las-stablecoins-y-para-que-sirven/

https://www.blockchain.com/charts/miners-revenue

https://www.blockchain.com/charts/total-bitcoins

https://www.ig.com/es/ethereum-trading/que-es-ether-y-como-funciona

https://www.kraken.com/es-es/learn/what-is-balancer-bal

Lau, D., Lau, D., Jin, T. S., Kho, K., Azmi, E., & Ong, B. (2020). *How to DeFi*. https://landing.coingecko.com/how-to-defi/

Leshner, R., & Hayes, G. (2018). *Compound : The Money Market Protocol*. 1–10.

Márquez Solís, S. (2016). *Bitcoin : guía completa de la moneda del futuro* . Ra-Ma.

Ocariz, E. B. (2018). *Blockchain y smart contracts : la revolución de la confianza* . RC libros.

Santiago Moreno, I. (2017). *La revolución de la tecnología de Cadena de Bloques en la economía: impacto en los distintos sectores económicos* . Editorial Académica Española.

Santiago Moreno, I. (2019). *La nueva economía blockchain y criptomonedas en 100 preguntas* . Ediciones Nowtilus.